OPTICAL HOMODYNE DETECTION AND APPLICATIONS IN QUANTUM CRYPTOGRAPHY

A DISSERTATION

SUBMITTED TO THE DEPARTEMENT OF COMMUNICATIONS &

ELECTRONICS OF TELECOM PARISTECH

IN FULFILLMENT OF THE REQUIREMENTS FOR

THE DEGREE OF DOCTOR

Jean-Marc Merolla (Université de Franche-Comté)	Rapporteur
Eleni Diamanti (CNRS LTICI)	Rapporteur
Patrick Bellot (TELECOM ParisTech)	Examinateur
Paul Voss (Georgia Institute of Technology)	Examinateur
Niclolas Pelloquin (SmartQuantum)	Examinateur
Francisco J. Mendieta (CICESE, Mexico)	Co-directeur de thèse
Philippe Gallion (TELECOM ParisTech)	Directeur de thèse

Qing Xu

2009

REMERCIEMENTS

Je tiens à exprimer toutes mes remerciements à toutes les personnes qui m'ont soutenu, aidé, encouragé, au cours de ces trois ans et sept mois de thèse.

Je remercie tout d'abord mon directeur de thèse, Professeur Philippe Gallion. La profondeur et la largeur de ses connaissances scientifiques et ses visions techniques m'ont bien aidé à réussir cette thèse. Son sens de l'humour et son intelligence m'ont inspiré dans les recherches scientifiques autant que dans la vie quotidienne. Cette thèse a aussi beaucoup bénéficié de la confiance et l'autonomie qu'il m'a accordée depuis le début.

Je tiens aussi ma gratitude à M. Francisco J. Mendieta, mon co-directeur de thèse, qui m'a beaucoup aidé pour les aspects scientifiques, les implémentations pratiques, et les analyses expérimentales. Sans lui, l'avancement de thèse aurait été beaucoup plus difficile. Je n'oublierai jamais sa passion pour le travail, sa gentillesse, et ses encouragements aux moments de réussite et d'échec.

C'est aussi un grand honneur pour moi d'avoir Paul Voss, Jean-Marc Merolla, Eleni Diamanti, Patrick Bellot, Nicolas Pelloquin dans mon jury de thèse, je les en remercie bien sincèrement pour leurs temps de lecture, lerus commentaires et surtout leurs critiques.

Mes plus sincères remerciements vont à Dr. Marcia B. Costa e Silva, avec qui j'ai commencé mes premières études et expériences en stage puis en thèse. Les deux ans de travail ensemble m'ont fait appris beaucoup d'expertise pragmatiste, et m'ont laissé également un bon souvenir pour toujours. Merci mon amie Marcia!

Je dois également citer Dr. Sébastien Agnolini, qui avait initié le système de cryptographie quantique et m'avait accompagné et aidé en stage et au début de la thèse. Ses travaux précédents et les instruments et composants acquis étaient indispensables pour mes progrès, Merci Sébastien!

Un grand remerciement à tous les collègues du département de Communications et Electronique qui ont travaillé avec moi: à Dr. Manuel Sabban pour son temps d'analyse sur la sécurité du système; à Dr. Sylvain Guilley qui m'a aidé à configurer les ports série des compteurs de photons; à M. Jean-Luc Danger qui m'a fourni généreusement les cartes FPGA pour piloter les modulateurs de phase; à M. Karim Ben Kalaia, le responsable du Laboratoire Electronique qui a aidé à fabriquer les cartes et interfaces électroniques; à M. Fréderic Pauget, ingénieur systèmes et réseau, qui m'a aidé à configurer les machines; à M. Alain Croullebois, le technicien responsable atelier mécanique, qui m'a aidé à fabriquer les plaques de modulateurs.

Je dois aussi remercier Dr. Arturo Arvizu Mondragón, chercheur de CICESE Mexique, qui a travaillé avec moi sur l'implémentation de la Costas Loop dans un récepteur homodyne conçu pour les états cohérents faibles.

Un grand merci aussi aux assistants et cadres administratifs: Chantal Cadiat, Danielle Childz, Marie Baquero, Zouina Sahnoune, Florence Besnard, et Stéphane Bonenfant, qui m'ont aidé à bien m'installer et travailler dans de bonnes conditions.

Je vous suis également reconnaissant aux professeurs du groupe communications optiques, Didier Erasme, Renaud Gabet, Guy Debarge, Yves Jaouen, et Cedric Ware, d'avoir répondu toutes mes questions techniques et organisé les séminaires du groupe au cours des ces années.

Je n'oublierais pas les collègues de bureau qui ont rendu ces années aussi agréables qu'enrichissantes: Sheng Yang, Ghassan Kraidy, Rym Ouertani, Eric Albert Bouton, Maya Badr, et Ali Osmane.

Finalement, je dois aussi remercier tous les amis à l'école qui m'ont soutenu aux moments difficiles et partagé ma joie: Vincent Lanticq, Philippe Hamel, Yang Liu, Shifeng Jiang, Juan Petit, Fausto Gomez Agis, Steevy Cordette, Mohammad Gharaei, Damien Fafchamps, Sami Mumtaz, Ishan Fsaifes, Waqqas Akhtar, Bruno Bristiel, Fabien Kefelian, Mounia Lourdiane, Hassan Teimoori, Charlotte Hucher, Aude Le Duc, Lina Mroueh, Michel Nahas, Mélanie Plainchault, Abdellatif Salah, Zhipeng Zhao, Laura Luzzi, Mireille Sarkiss, Amira Alloum, Davi Bibiano Brito, Michael Grelier, Fabrice Linot, Judson Braga, Antoine Khy, Francisco Vidal, Sami Mekki, Korinna Lenz, Manel Ben Romdhane, Alban Gruget, Chadi Jabbour, Joao Francisco Ribeiro Negrao, Denis Teixeira Franco, Maí Correia Rabelo de Vasconcelos, Daniel Comalrena, Antonio Cipriano, Emilio Calvanese Strinati, Ioannis Krikidis, Hicham Ezzat, et David Camarero, et touts les autres qui me pardonnerons de les avoir oubliés.

RESUME FRANÇAIS

CONTEXTE SCIENTIFIQUE

Les réseaux et systèmes de télécommunications mondiaux fondent aujourd'hui leur confidentialité sur la cryptographie classique, afin de garantir le secret nécessaire aux gouvernements (défense, sécurité du territoire), aux sociétés civiles et aux citoyens, notamment dans le cadre des transactions par Internet. La sécurité proposée par le chiffrement symétrique moderne, basée sur la difficulté de rechercher exhaustivement la clef de déchiffrage, reste construite sur des hypothèses mathématiques fragiles. En effet, une percée brutale, mais possible, en mathématiques ou dans le domaine des calculateurs, peut effondrer cette confiance et rendre les messages actuellement échangés, et ceux qui le sont déjà, lisibles. Quand bien même ces crypto-systèmes devraient rester sûrs, il est difficile de distribuer confidentiellement des clefs aux utilisateurs. En conséquence, dans la plupart des systèmes actuels, les clefs utilisées pour une transaction reposent souvent sur une clef de « grande longévité », rarement changée, alors que la sécurité n'est garanti que pour des clefs à l'usage unique (One Time Pad). Par conséquent, le problème principal est devenu la génération et de la distribution de clefs. Sa solution permettrait de fournir une sécurité démontrée, augmentant considérablement la sécurité actuelle.

La distribution quantique de clef (QKD) est aujourd'hui la seule manière connue de distribuer des clefs avec une sécurité inconditionnelle. La sécurité quantique résulte en premier lieu de l'impossibilité de dupliquer les signaux reçus, principe de non-clonage, ou d'en distraire une partie significative sans signer son intervention par une modification importante du taux d'erreur des signaux reçus. La sécurité repose en second lieu sur le caractère destructif ou perturbateur de toute observation et sur les erreurs résultant d'observations incompatibles d'un même objet quantique. Il s'agit par exemple de la mesure de la polarisation ou de la phase d'un photon unique sur deux bases différentes, ou comme la mesure simultanée des deux quadratures d'un même état cohérent contenant plusieurs dizaines de photons. Un taux d'erreur contrôlé garantit alors, a posteriori, la confidentialité de la liaison. La sécurité peut également reposer, selon le type de protocole choisi, sur des super corrélations quantiques ou corrélation EPR, ou encore intrications. Une grande diversité d'implémentations de la « couche quantique » est donc possible.

La distribution quantique de clef (QKD) utilise donc, sous des formes variables, les propriétés quantiques pour fournir des moyens de détecter une écoute indiscrète. Une telle écoute clandestine est discernable, par les parties souhaitant convenir d'une clef, parce que l'oreille indiscrète perturbe nécessairement, en le mesurant, l'état de la lumière transmise. Une fois la clef distribue, les parties peuvent obtenir le secret parfait sur des données en employant un bit de clef pour chaque bit de données envoyées. D'autres méthodes de chiffrage sont possibles également.

Bien que les travaux expérimentaux dans le domaine de la QKD aient effectué des progrès considérables, il subsiste de nombreux problèmes avec des systèmes actuels. Les plus rapides d'entre eux, fournissant un débit net de clef supérieure à 1 Mb/sec, ne sont ni fiables ni pratiques d'utilisation. Par ailleurs les premiers systèmes de QKD actuellement disponibles dans le commerce ne sont ni rapides ni souples. En vérité, il n'existe encore aucun système actuel pouvant vraiment satisfaire à la demande, aux conditions d'environnement et à la gestion de réseaux de télécommunications actuels. Ce travail de recherche exploratoire a pour ambition d'apporter une solution, sinon des éléments de solutions significatifs, à cette problématique en s'attaquant aux principales limitations actuelles :

- Augmenter la **fiabilité** d'une intégration verticale, de la couche physique à la couche applicative sur IP. Le système sera assez robuste pour résister à des modifications, changements ou progrès, de la couche quantique et pourra ainsi servir de plate-forme évolutive et polyvalente, adaptable aux différentes de réalisations de couche physique par un niveau réglable de sécurité.

- Augmenter la **flexibilité** en permettant une « sécurité sur demande » autorisant à des clients de choisir dynamiquement le niveau de la sécurité adapté à leur besoins et en envisageant son implémentation dans un contexte WDM et multi utilisateur.

- Augmenter la **rapidité** et l'efficacité en explorant les marges d'amélioration de vitesse d'horloge et de rendement de production de clef brute.

- Augmenter la **robustesse** par l'utilisation de mécanismes de synchronisation et de contrôle avancés et des codes atteignant la sécurité maximale lors des processus de réconciliation, de correction d'erreur et d'amplification de secret et permettant d'économiser la liaison symétrique nécessaire à la distillation de la clef finale.

Ce travail de thèse vise donc à combler de manière polyvalente le gap, en termes de vitesse, fiabilité et robustesse, entre les possibilités offertes par une implémentation possible de la couche quantique (Protocole BB84 avec codage temporel), et les exigences en matière de clef des systèmes et des applications actuelles.

CONCEPTION ET REALISATION D'UN SYSTEME QKD

Les communications, sur un canal non protégé, imposent l'échange d'une clef entre Alice et Bob qui sont, avec Eve, tentant d'obtenir cette clef à leur insu, les acteurs incontournables de tout scénario cryptographique.

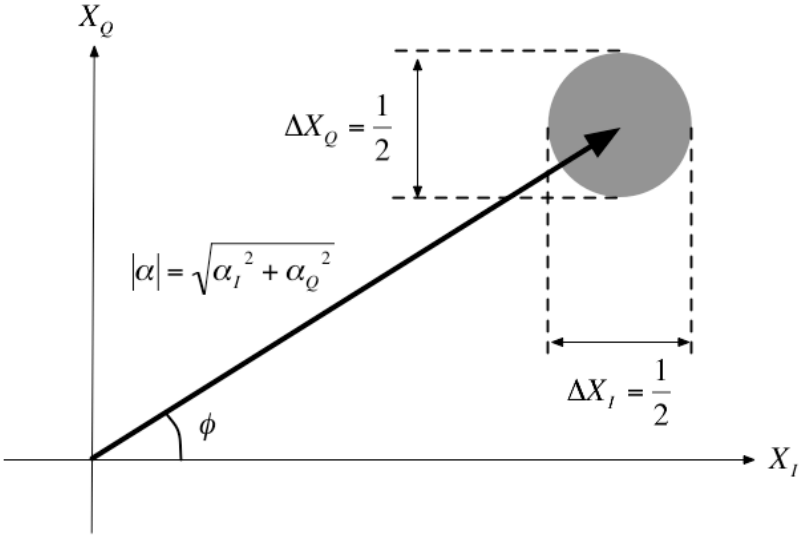
Si la physique quantique nous permet de construire des liens inconditionnellement sûrs, cette construction est, outre les difficulté technologiques, entravée par trois facteurs. Le premier, auquel nous nous proposons de répondre, est le problème de la sensibilité aux attaques de type « l’homme au milieu (man in the middle) ». Le deuxième est une longueur de lien restreinte, typiquement quelques kilomètres à quelques dizaines de kilomètres. Le troisième, crucial, est l’incapacité technologique actuelle à fournir des répéteurs et des routeurs quantiques capable de réexpédier les objets quantiques sans les mesurer.

Le protocole de cryptographie quantique sous la forme initialement proposée par Bennett et Brassard (BB84) utilise la polarisation (spin des photons) et l’impossibilité d’une mesure informative dans une base conjuguée. La nécessité de maintenir ou de contrôler la polarisation est un handicap à son implémentation sur des liaisons à fibre optique ne maintenant en général pas la polarisation.

L’utilisation de la phase optique, réputée très vulnérable aux non linéarités est envisageable dès lors que des signaux très faible et/ou d’enveloppe constante sont transmis et qu’une réception sensible à la phase utilisée. Cette dernière peut être réalisée par interférométrie au prix de la réalisation et de la stabilisation d’un interféromètre pour une démodulation cohérente. Les contraintes de polarisation, qui n’est plus porteuse de l’information, sont alors relaxées.

L’utilisation de modulateurs de phase optique et l’utilisation de la phase d’une modulation par sous porteuse ont donné lieu à une démonstration convaincante au prix de circuits et d’une synchronisation radio fréquence complexes. L’utilisation de ce type de modulateur permet une implémentation directe sur la phase optique.

En absence actuelle de source performante générant des photons sous forme d’état de nombre à 1 photon, il est usuel d’employer les états cohérents. Un état cohérent $|\alpha\rangle$ est représenté sur la Figure 1, ou le cercle grisée représente les incertitudes quantiques, il n’y a pas de distinction intrinsèque à l’une des deux quadratures, et leur incertitude est identique $\Delta X_I = \Delta X_Q = \frac{1}{2}$.



X_Q
$\Delta X_Q = \frac{1}{2}$
$|\alpha| = \sqrt{\alpha_I^{\,2} + \alpha_Q^{\,2}}$
$\Delta X_I = \frac{1}{2}$
ϕ
X_I

Figure 1 Vecteur de Fresnel d'un état cohérent $|\alpha\rangle$

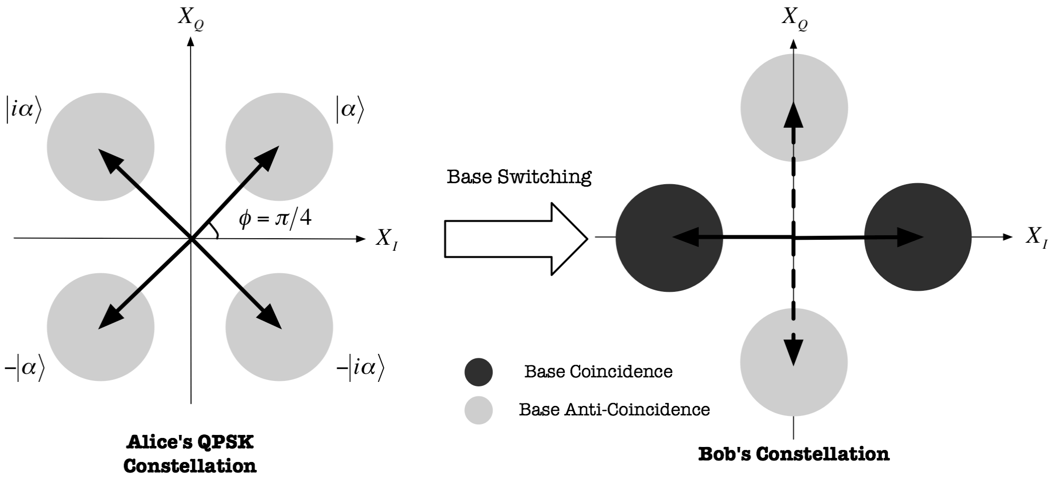


Figure 2 La conversion de constellation QPSK en une constellation BPSK

Nous proposons donc une implémentation du protocole BB84 utilisant les états de phase d'état cohérent dans deux bases orthogonales, soit deux symboles dans chaque base. Le récepteur homodyne pour les applications QKD doit être conçus de manière à compenser les fluctuations de phase et de polarisation dans les interféromètres, ainsi que dans le reste du canal de propagation.

Si l'état de polarisation du signal optique reçu ne joue aucun rôle dans des récepteurs de détection directe, simplement parce que le photo-courant généré en ces récepteurs ne dépend que du nombre de photons incidents, ce n'est pas le cas pour les récepteurs cohérents, dont le fonctionnement nécessite que l'état de la polarisation de l'oscillateur local corresponde bien à celui du signal reçu. L'exigence d'un accord de polarisation et sa réalisation supposée autorise une représentation scalaires des champs E_S et E_{LO}. Cet accord se réalise, pour les deux champs optiques, à l'aide des composants de maintien de polarisation, tels que les fibres dites PM, et les séparateurs/combinateurs de polarisation. L'interférence de E_S et E_{LO} étant utilisée, et un circuit de décision permet de reconstituer le flux de bits transmis. Tout changement différentiel dans de l'état de polarisation réduit le signal utile et affecte les performances du récepteur. Dans le cas limite où les états de polarisation E_S et E_{LO} sont orthogonaux, le signal d'interférence disparaît.

Le retard relatif, entre l'impulsion du signal et l'impulsion de la référence, introduit dans l'interféromètre doit rester stable afin de permettre un fonctionnement correct d'un système QKD, sujet à des variations de température, et des vibrations mécaniques. Dans une de nos expériences, une variation de phase de 6π a été enregistrée sur une période de 16 heures.

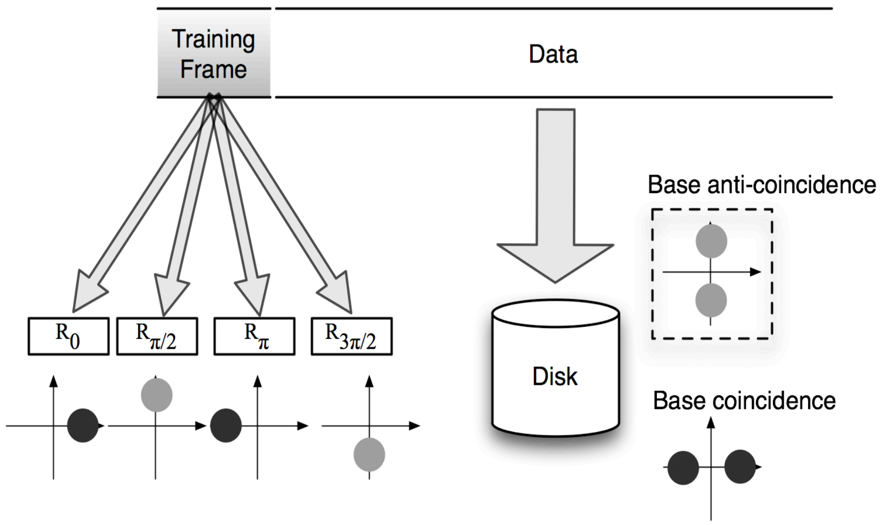


Figure 3 Séquence d'apprentissage et séquence de données

La correction de erreur de phase en temps réel pourrait se réaliser sur l'interféromètre de Bob par l'insertion d'une fibre soumise à une contrainte contrôlée (fiber-stretcher), ou bien par l'ajustement de phase sur le modulateur Bob. En effet, notre méthode consiste à insérer périodiquement des séquences d'apprentissage entre les séquences des données, afin de calculer la variation de phase et de la compenser via le fiber-stretcher.

DETECITON DE BITS QUANTIQUES

Les compteurs de photon, exploitant le courant avalanche déclenché par un photon incident sur une jonction P-N inversement polarisée afin de détecter un rayonnement incident, sont spécifiquement conçus pour fonctionner avec une tension inverse bien au-dessus de la tension de claquage. Dans la bande des télécommunications, les compteurs de photons fonctionnant en mode Geiger sous un contrôle très précis de basse température, présentent un faible rendement quantique, un taux de coup d'obscurité (dark count) élevé, ainsi qu'un effet d'échos après impulsion (afterpulse). Les systèmes utilisant les compteurs de photons ont, aujourd'hui, une limitation de la fréquence de répétition à 4 ou 8 MHz.

D’autre part, en cherchant un taux de génération de clé plus élevé, la détection homodyne équilibrée (BHD) utilisant les photodiodes PIN, et le gain de mélange d’un oscillateur local (LO), peut constituer une alternative intéressante. Dans BHD une seule quadrature étant mesurée, il n’y a pas de bruit intrinsèque supplémentaire aux fluctuations de point zéro du champ signal. Le bruit quantique du signal d’entrée est, dans ce cas, la seule limitation et le bruit du LO n’a qu’une influence négligeable. Un LO de grande puissance permet d’avoir un gain de mélange assez important. En outre, la BHD utilisant les photodiodes PIN conventionnelles présentent une efficacité quantique beaucoup plus importante et un temps de réponse beaucoup plus court que les compteurs de photons, de plus son utilisation est considérablement plus simple dès lorsque la génération et la stabilisation de l’oscillateur local sont acquises.

Etant donné un champ signal faible E_S et un champ LO fort E_{LO} ($|E_{LO}| >> |E_S|$), la technique BHD peut affranchir certains effets non souhaitable des compteurs de photons. La post-détection, le filtrage, le seuil de décision et la synchronisation des symboles doivent tout être cependant conçus car le processus de décision est effectué a posteriori, contrairement aux produits commerciaux de comptage de photons qui incluent un circuit de décision intégrée, qui est un difficile compromis entre l’efficacité de détection et le taux de coup d’obscurité. En outre BHD conduit à un taux d’erreur binaire (BER) classique, tandis que le comptage de photons qui en théorie ne présentent que des effacements et des coups d’obscurité génèrent un taux d’erreur binaire quantique (QBER).

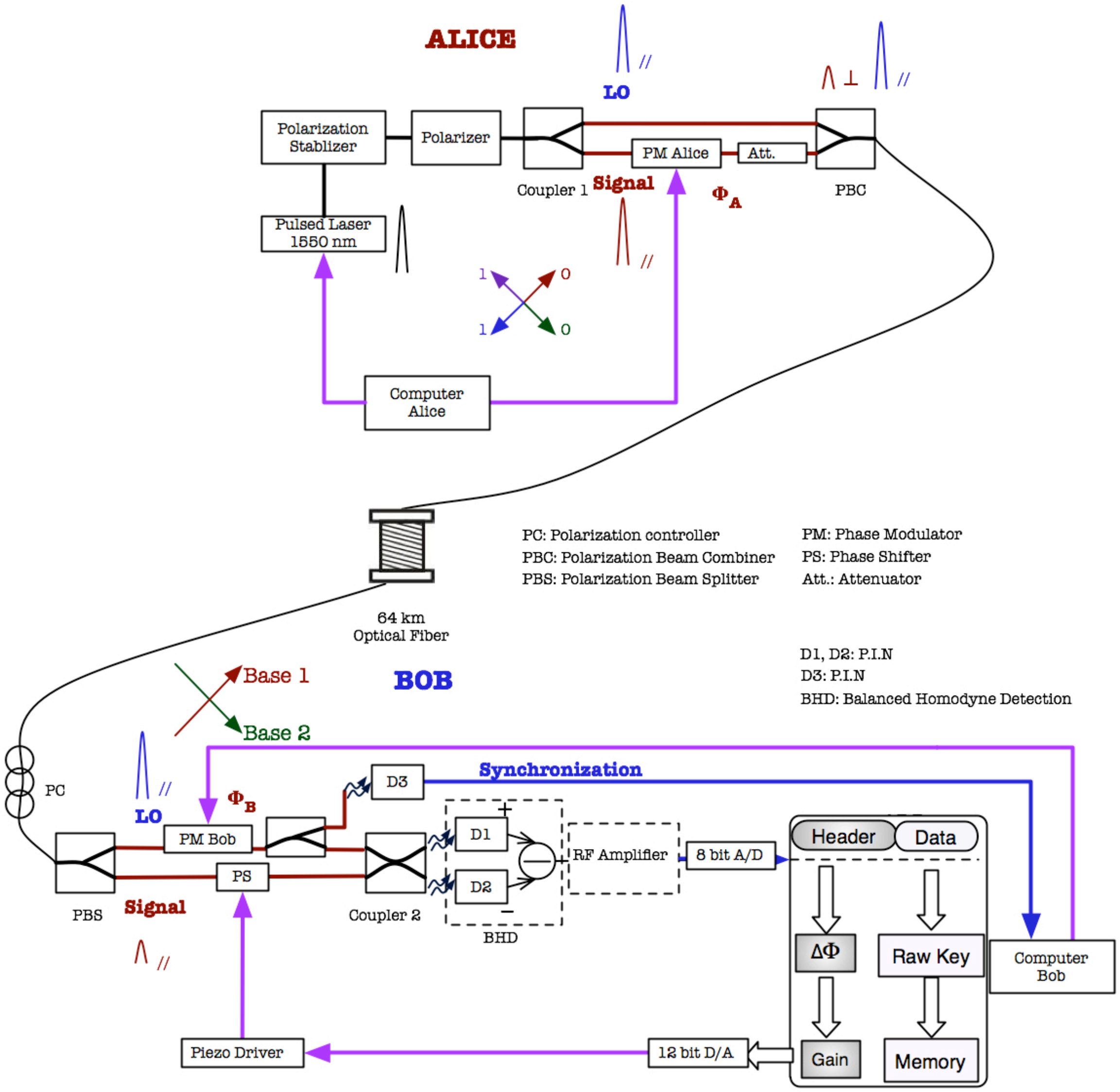


Figure 4 Schéma expérimental

Nous avons mis en œuvre un dispositif expérimental de système QKD en modulation QPSK qui fonctionnant avec un trajet unique et un sens de parcours aller simple. Les deux techniques de détection, comptage de photons (PC) et détection homodyne équilibrée (BHD) ont été mis en place. Un arrangement souple a été conçu de telle sorte que seuls de légers changements soient à faire pour passer de la technique de détection de PC à BHD.

Nous utilisons une source laser ILM électro-absorbant (laser integrated modulateur, AVANEX) à 1550nm pour générer des impulsions de largeur 5ns avec un taux d'extinction en intensité à 18 dB. A la détection PC, la fréquence de fonctionnement est limitée à 4MHz, tandis qu'à la détection BHD, la fréquence de répétition peut monter jusqu'à dizaines de GHz avec les composants disponibles d'aujourd'hui. Pourtant la comparaison parallèle, nous avons choisi d'utiliser dans un premier temps, une fréquence d'opération de 4MHz afin de tester les performances du récepteur PC et du récepteur BHD.

Une méthode de séparation de polarisation est utilisée dans notre arrangement en vue d'améliorer l'isolation entre l'impulsion signal et l'impulsion référence forte, car le taux d'extinction de 18 dB en intensité seul ne suffit pas pour le multiplexage temporel des impulsions de signaux et de LO. Chez Alice les impulsions laser sont séparées via un séparateur de polarisation (PBS) avec un taux d'extinction de 25 dB, la composante horizontalement polarisée passe par le bras LO et la composante verticalement polarisée passe par le bras Signal de l'interféromètre Mach-Zehnder, qui est construit avec les fibres de maintien polarisation (PM).

Alice encode ses impulsions Signal (Φ_A: $\pi/4$ et $-3\pi/4$ en base A_1 : $-\pi/4$ et $3\pi/4$ en base A_2) avec un modulateur de phase, générant une modulation QPSK. L'impulsion Signal et l'impulsion LO non-modulée sont multiplexées en temps avec un combinateur de polarisation (PBC), ainsi que le décalage entre les deux impulsions sont bien ajustées à 20ns, soit 4 mètres de fibre optique. Le fait que l'impulsion signal et l'impulsion LO soient polarisées orthogonalement permet d'avoir un taux d'isolation suffisamment élevé dans le canal de propagation. Un atténuateur optique est également utilisé pour réduire les impulsions signal au niveau quantique.

Les impulsions combinées Signal-LO passent ensuite dans une fibre SMF. Coté récepteur Bob utilise un autre PBS pour séparer les impulsions LO et les impulsions Signal. Une petite partie d'impulsion LO est prélevée par une autre photo-diode PIN D3 afin de fournir le signal de synchronisation.

Le récepteur Bob consiste à une structure interférométrique similaire à celui de l'émetteur Alice. Il effectue la modulation de phase sur LO, en appliquant ses choix de base sur un modulateur de phase Niobate de Lithium (Φ_B: $\pi/4$ in Base B_1, $-\pi/4$ in Base B_2). Le délai entre l'impulsion Signal et l'impulsion LO est soigneusement ajusté à 20ns afin d'optimiser leur recouvrement sur les deux ports d'entrée du coupleur PM, au même état de polarisation (POS).

Nous utilisons un convertisseur A/D de 8bits pour l'acquisition des symboles. La mesure de quadrature est proportionnelle à $\cos(\Phi) = \cos(\Phi_A - \Phi_B)$: la coïncidence de base (BC) se produit lorsque $\Phi = 0$ or π; l'anti-coïncidence de base (AC) se produit lorsque $\Phi = \pm\pi/2$.

La variation de phase $\Delta\Phi$ est compensée via un déphaseur (PS) optique. Nous utilisons des trames d'apprentissage périodiques qui entrelacent avec les trames des données, afin de calculer le changement de phase du système et de réagir sur le PS dont la tension de déphasage π vaut $V_\pi = 10V$. Un driver externe de Vp-p = 160V permet d'avoir une dynamique de $[-8\pi, 8\pi]$ et un temps de réponse de quelques millisecondes. Le système réinitialise automatiquement à zéro lors de l'atteinte des limites. Dans nos expériences, l'erreur de phase résiduelle s'est réduite à moins de 5 degrés même avec un signal de très faible niveau.

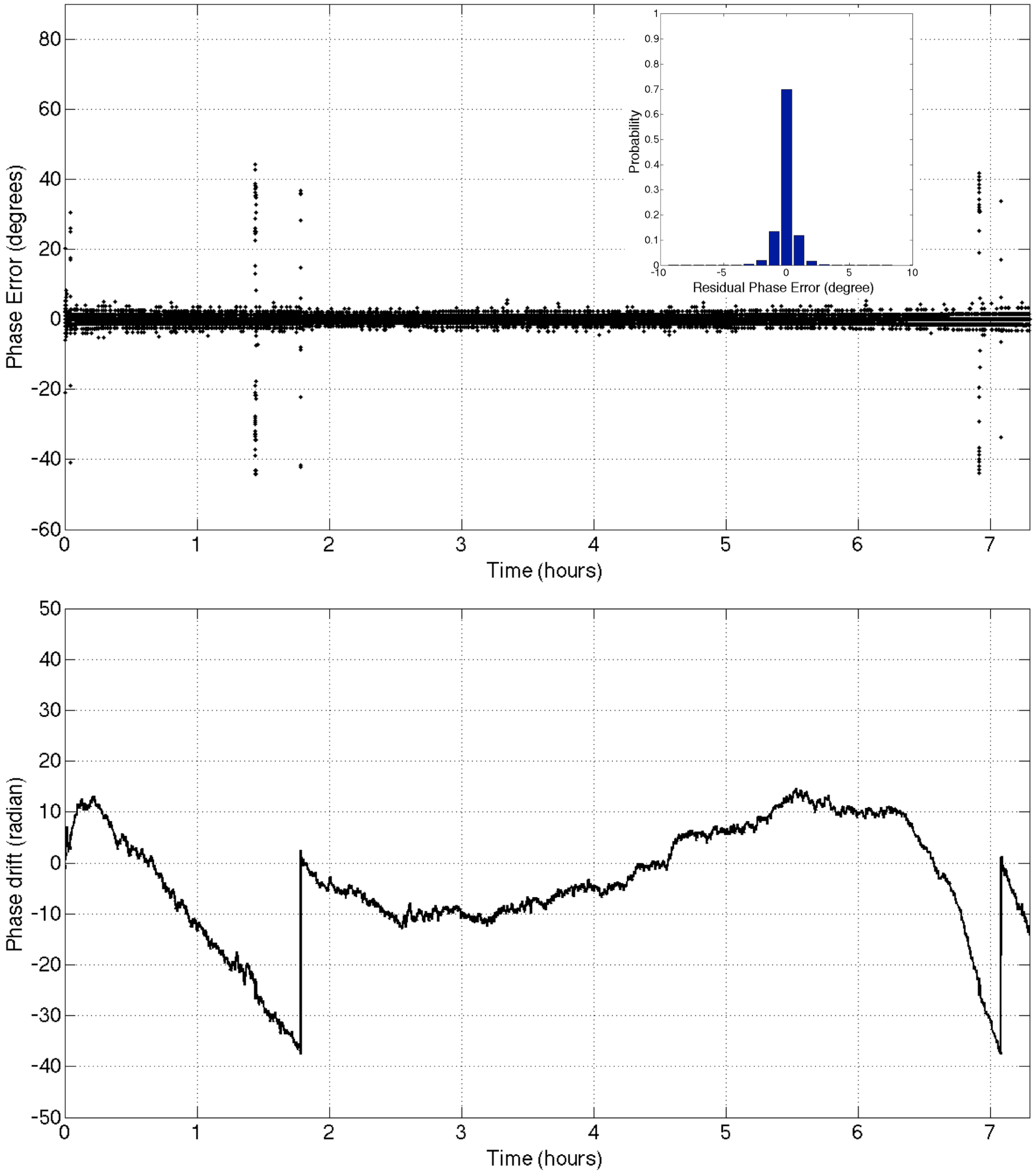


Figure 5 L'erreur de phase résiduelle de notre système QKD

La détection homodyne permet que l'encodage du signal en phase soit plus adapté que l'encodage en polarisation pour les transmissions par fibre optique. Dans un tel système, la récupération de phase optique et celle de l'information portée doivent être résolues simultanément par Bob et Eve qui ont l'accès au canal physique. Toutefois, un processus de décision est obligatoire côté récepteur, car les différents états cohérent transmis par des sources de lumière cohérente ne sont pas orthogonaux, et qu'une simple mesure de projection Von Neumann ne permet pas de distinguer les états avec une certitude, ce qui induit à un taux d'erreur intrinsèque, comme le montré dans la Figure 6 (a). Dans un système QKD l'effacement de bits dû à l'absorption du canal, ou bien plus généralement par la décision d'abandon, peut se gérer au cours du processus de réconciliation et se transforme en une réduction du taux de génération brut de clé.

En résumé, nous donnons ici une comparaison récapitulative du récepteur interférométrique à annulation de champs utilisant les compteurs de photon (PC), et le récepteur homodyne équilibré (BHD) à fort niveau d'oscillateur local (LO) utilisant des photodiodes PIN :

- La configuration PC présente une bande passante de 4MHz et une sensibilité quantique de l'ordre 10%. En effet, bien qu'en divisant l'amplitude du signal reçu sur chaque détecteur, contrairement à un séparateur de polarisation, le signal sur le détecteur actif y est plus élevé, grâce à l'abonnement produit par l'oscillateur local. Ce récepteur ne permet cependant pas d'atteindre la sensibilité du récepteur de Kennedy, bénéficiant du même abondement, à cause de la division de l'amplitude du signal par le coupleur symétrique. Il n'y a en théorie que des effacements équidistribués sur les deux symboles, mais en pratique les erreurs sont produites par les imperfections des compteurs de photons.

- La configuration BHD permet une fréquence d'opération beaucoup plus élevée, et une sensibilité quantique de l'ordre de l'unité, ainsi que le gain de mélange du LO permet de s'affranchir du bruit et des effets thermiques. Un taux d'erreur intrinsèque résultant des fluctuations du vide qui entrent par le port signal approche assez facilement en pratique la limite quantique standard (SQL).

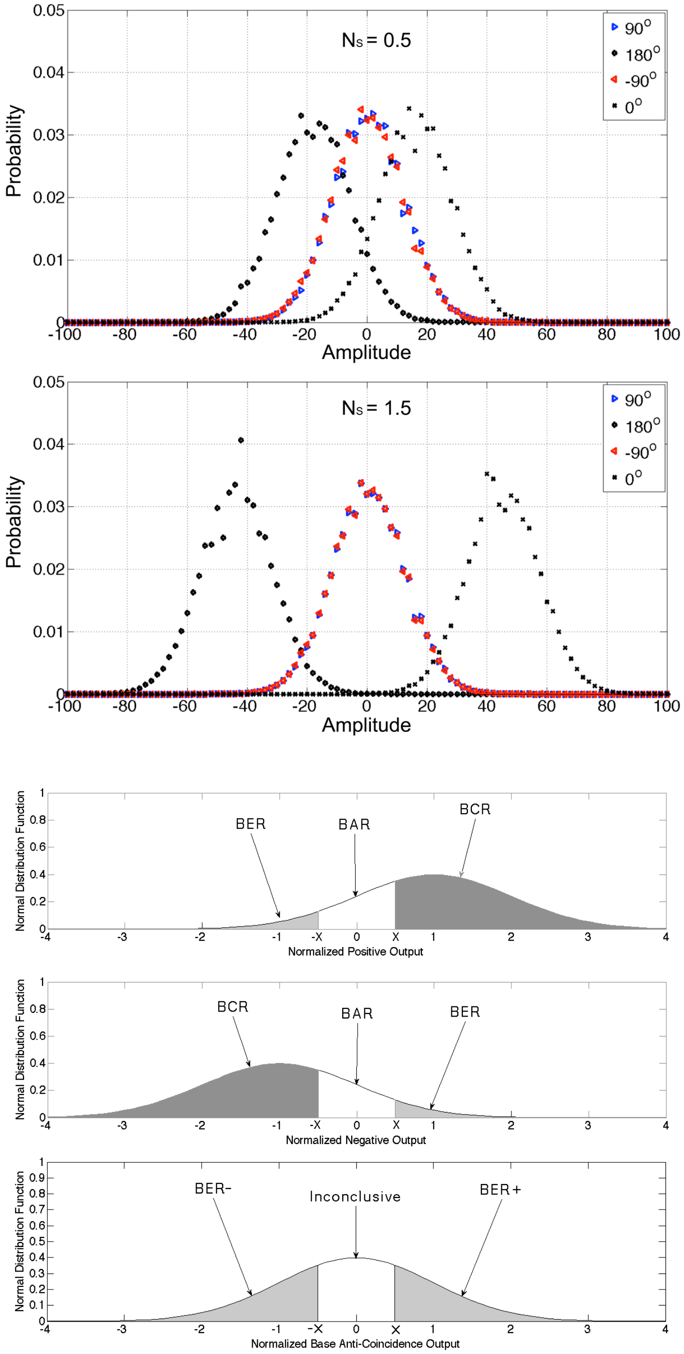


Figure 6 a) Histogrammes de signaux détectés avec nombre de photon moyen par bit N_S = 0,5 et 1,5; b) Décision BHD avec double seuil -X et X.

La détection homodyne BHD peut également se mettre en œuvre en utilisant des seuils de décision pour les signaux électroniques. Un tel système QKD en codage de phase a été proposé initialement par le groupe de Hirano. Nous avons ainsi choisi d'élaborer notre système en implémentant une décision à double seuil. Pour la discrimination du signal Bob met en place deux seuils -X et X, comme le montré la Figure 6 (b). Bob juges le bit comme le 1 lorsque x > X et le 0 lorsque x < -X, noté BCR (bit correct rate); sinon la décision sur ce bit est abandonnée, noté BAR (bit abandon rate).

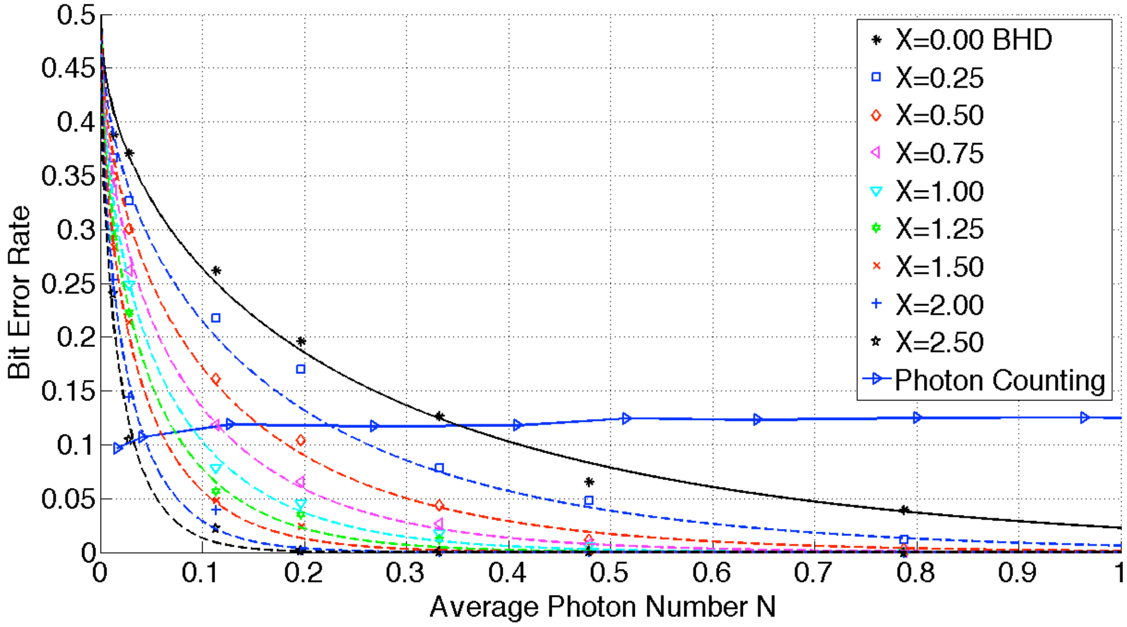


Figure 7 Post-détection BER de BHD et QBER de comptage de photons

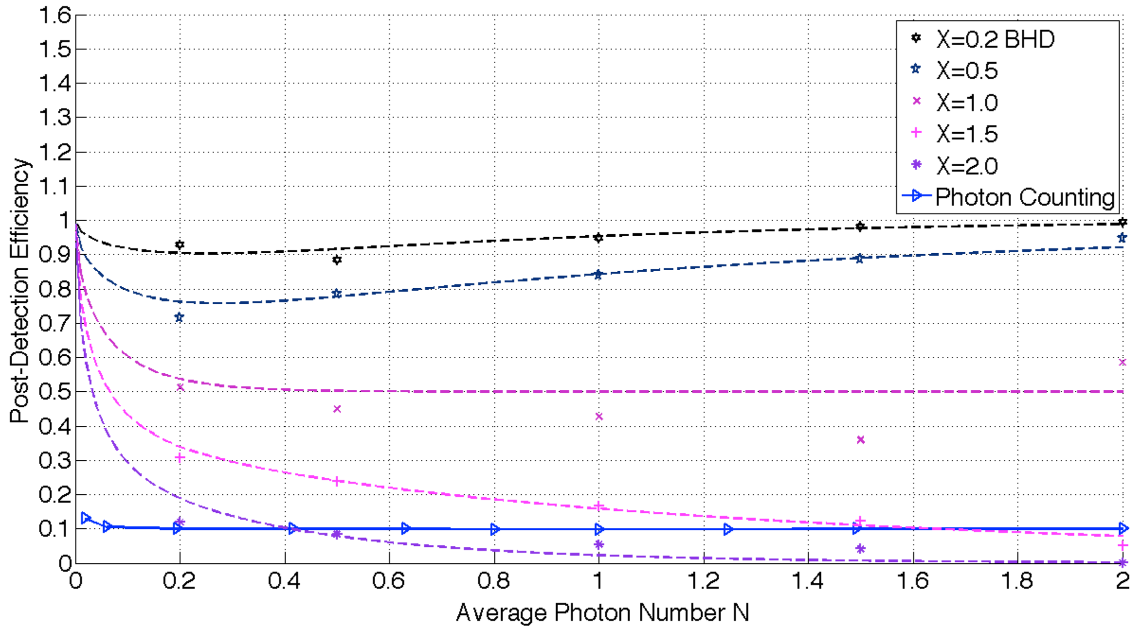


Figure 8 Mesures expérimentales de l'efficacité de détection

Comme nous montrons dans les Figures 7 et 8, la mise en œuvre d'un processus de décision à double seuil conduit à des mesures non-conclusives, et une perte d'efficacité de génération de clés, afin réduire le BER de post-détection. Son efficacité reste cependant en générale bien plus élevée que celle des compteurs de photon à la longueur d'onde 1550nm. En fait, l'attaque d'Eve entraîne plus souvent une dégradation du signal chez Bob que d'une substitution, ce qui suggère que l'effacement de bit soit plus efficace que la suppression simple des symboles de anti-coïncidence de base, qui est indépendante de l'intervention de Eve.

SECURITE DE SYSTEME QKD

Afin d'étudier la sécurité d'un système de cryptographie quantique, nous procédons à prendre en compte l'action d'Eve et analyser la quantité d'informations qui lui est accessible. Nous représentons les entropies d'information d'Alice, de Bob et d'Eve par *H(A)*, *H(B)* et *H(E)*, respectivement. L'entropie conditionnelle de Bob et Eve est définie comme $H(A|B)$ et $H(A|E)$, respectivement, en supposant que l'information d'Alice est connue.

Les informations mutuelles *I(A,B)*, *I(A,E)* sont définies comme l'estimation de la quantité d'information partagée par Alice et Bob, et celle partagée par Alice et Eve, respectivement. Il faut noter qu'Eve est considérée seulement limitée par les lois de la physique.

La clé est dite sécurisée si *I(A,B)* est supérieure à *I(A,E)*. Cependant, sous certaines attaques comme le prélèvement de photon ou photon-number-splitting (PNS), l'espion Eve peut obtenir de larges connaissances sur la clé établie entre Alice et Bob, par conséquent, la détection d'Eve est particulièrement importante surtout pour les transmissions longue distance. Au cours du processus de génération de clés, Bob doit discerner en temps réel les variations de BER_P de manière à percevoir les attaques d'Eve et de garantir la sécurité.

La Figure 9 montre que le taux d'erreur de post-détection BER_P est largement modifié dans le cas de l'attaque de type interception-renvoi, de l'attaque par base intermédiaire, ainsi que l'attaque de PNS. Comme nous soulignons que dans le cas de l'attaque interception-revoi, Bob peut sélectionner une valeur X élevée afin de maintenir le gain d'information sur Eve, alors aucun gain d'information ne peut être obtenu sous les attaques de base intermédiaire ou de PNS. Dans ces cas-là, Bob peut discerner les attaques d'Eve en comparant le BER_P opérationnel et le BER_P théorique. Dans le cas d'une attaque plus avancée PNS étendue (extended PNS attack), qui est proposée par Lütkenhaus, Eve est supposée capable de cacher sa présence en prélevant uniquement un photon dans les impulsions de multi-photons, un protocole de multi-états similaire à états de leurre (Decoy States) peut s'employer afin d'observer les variations d'efficacité de détection ρ en utilisant des impulsions de nombre de photon variables.

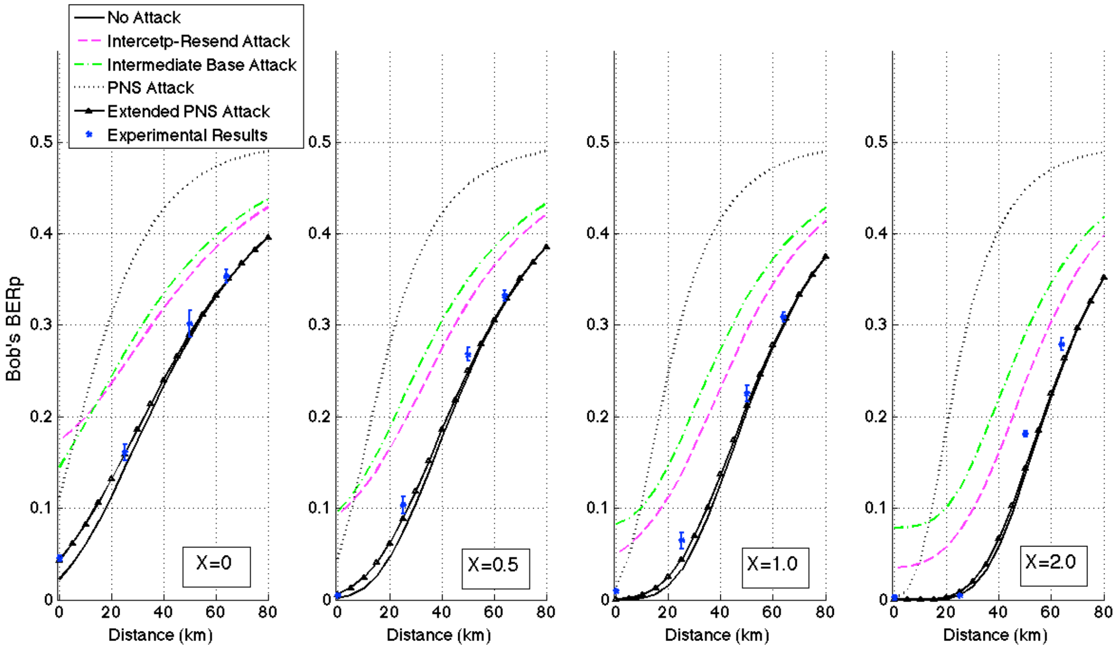


Figure 9 Post-détection BER_P sous diverses attaques

TABLE OF CONTENTS

LIST OF TABLES

Number *Page*

LIST OF FIGURES

Number *Page*

CHAPTER 1   INTRODUCTION

Moore’s Law describes an important trend in the history of computer hardware: the number of transistors that can be inexpensively placed on an integrated circuit is increasing exponentially, doubling approximately every 18 months [1]. The trend has continued for more than half a century and is not expected to stop for a decade at least and perhaps much longer. This has dramatically changed the usefulness of digital electronics in nearly every segment of the world economy. It is also a main driving force of technological and social changes in the late 20th and early 21st centuries thanks to the ongoing boom of information technology (IT) and telecommunications infrastructure. Meanwhile, the information security that protects information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction is much more than just a concern of privacy, confidentiality and integrity.

Cryptography, etymologically derived from Greek κϱυπτός kryptós “hidden”, and the verb γϱάφω gráfo “write” or λεγειν legein “speak”, is generally be defined as the art of enciphering (encryption) and deciphering (decryption) messages to hide the information carried by the message. A cipher is a pair of algorithms that perform this encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm, and in each instance, by a key. This is a secret parameter, i.e. ideally known only to the communicators, for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes.

The security of the conventional public-key cryptosystems such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. It is threatened by the calculation capacity of the super computer, or eventually the quantum computer. On the other hand, information theory shows that the traditional private-key (secret-key) cryptosystems cannot be totally secure unless the key is used once only, and is at least as long as the enciphered text. This algorithm is also called one-time pad (OTP) or Vernam code[2].

Based on the foundations of quantum mechanics, in contrast to traditional public key cryptography, the quantum cryptography's (QC) important and unique property is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge from the key [3-6]. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superposition or quantum entanglement, transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a given threshold a key can be produced and guaranteed as secure, otherwise no secure key is possible and communication is aborted.

Another important point is that QC is only used to produce and distribute a key, not to directly transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with quantum key distribution (QKD) is OTP, as it is provably unbreakable when used with a secret, random key.

Optical QKD system may be ideally based on the use of single-photon Fock states in which any state of the Fock space is with a well-defined number of particles. Unfortunately, these states are difficult to realize experimentally. While waiting for a reliable single photon source, a more practical choice of our days is faint laser pulses [7-9] or entangled photon pairs [10,11], in which both the photon and the photon-pair number distribution, obey the Poisson statistics [4].

The implementation of a QKD system depends essentially on the detection of single photon, the carrier of the key elements. Today, the single photon avalanche diode

(SPAD) are widely used. SPAD works in Geiger gated-mode under precise temperature control, i.e. around -30ºC, and exhibits inherent low quantum efficiency around 0.1, the inevitable dark count and residual after-pulse noise due to the macroscopic avalanche [12,13] at telecom wavelength (1550 nm). Furthermore its operational frequency is limited to 4-8MHz due to the necessary quenching process.

Coherent optical communication is one of the most promising ways to achieve highest receiver sensitivity, excellent spectral efficiency and longest transmission span for the next generations of optical communication systems. Already in the late 1980s and early 1990s coherent systems attracted a lot of attention [15-27] as it was a promising way to improve the receiver sensitivity. In the race for speed and distance, balanced homodyne detection (BHD) scheme using positive-intrinsic-negative diode (PIN) constitutes an efficient receiver scheme for the QKD system.

BHD, when used with a local oscillator (LO) of suitable power for the operation near the quantum noise limit, provides the mixing gain to overcome the thermal noise [9]. The conventional PIN photodiodes operating at room temperature present much higher quantum efficiency and response speed, and lower noise as compared to the gated photon counters. As well its cost is much lower and the supply requirements are much simpler.

Post-detection, filtering, threshold and symbol synchronization stages must be properly designed as in BHD the decision process is carried out *a posteriori* and the threshold can be carefully adjusted for a tradeoff between the key generation efficiency and the dark count rate, which is opposed to photon counting scheme that inherently performs built-in decision. Additionally BHD leads to classical bit error rate (BER) while only quantum bit error rate (QBER) is considered in photo counting.

In chapter 2 we first review the principles of the QKD system, including the BB84 protocol, key-encoding schemes, and in chapter 3 we discuss the fundamental physical challenges in QKD system implementations.

In chapter 4 we recall the principles of the coherent detection system, as well as its major noise sources, and the other technical impairments in a balanced homodyne receiver. In chapter 5 we describe the nature of weak coherent states (WCS) and the QPSK phase encoding for QKD applications based on quantum mechanics.

In chapter 6 we introduce the optical and electronic components that are used in our experimental QKD setups and we demonstrate the technical methods to overcome the system impairments, followed by the first QKD system validation.

In chapters 7 and 8 we introduce the two receiver structures for the QKD system. We present the experimental arrangements of the one-way BB84 QKD system using WCS pulses, i.e. QPSK format encoding at the sender Alice's end and BPSK down-conversion at the receiver Bob's end. Photon counting and BHD [16, 17, 18] schemes are implemented with system impairments compensation using training frames, for both the phase synchronization and polarization mismatch. Next we compare the system performances of the two detection schemes in terms of detection efficiency and BER. We also analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack.

Finally in chapter 9, we demonstrate a synchronized feedback homodyne detection system for WCS by minimizing the real-time phase error, using sequential in-phase and in-quadrature (I-Q) measurements as the inputs of a synthetic digital Costas phase-locked-loop (PLL). We report the experimental results of I-Q uncertainty measurements and we also demonstrate a method for the reconstruction of Wigner function from 128 equidistant phase states histogram measurements by applying the inverse Radon back-projection function.

REFERENCES

1. G. E. Moore, “Cramming more components onto integrated circuits”, *Electronics* **38**, 114--117(1965).
2. G. Vernam, “Ciper printing telegraphe systems for secret wire and radio telegraphic communications”, *Journal American Institute of Electrical Engineering* **55**, 109--115 (1926).
3. C. H. Bennett, and G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, *Proceeding of IEEE International Conference on Computers, systems, and Signals Processing*, 175--179 (1984).
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, *Reviews of Modern Physics* **74**, 145--195 (2002).
5. T. P. Spiller, “Quantum information processing: cryptography, computation, and teleportation”, *Proceedings of the IEEE* **84**, 1719--1746 (1996).
6. C. H. Bennett, and P. W. Shor, “Quantum information theory”, Invited Paper *IEEE Transactions on information theory* **44**, 2724--2742 (1998).
7. J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, H. Porte, and W. T. Rhodes, “Phase-modulation transmission system for quantum cryptography”, *Optics Letters* **24**, 104--106 (1999).
8. F. Grosshans, and P. Grangier, “Continuous variable quantum cryptography using coherent states”, *Physical Review Letters* **88**, 057902 (2002).

9. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection", *Physical Review A* **68**, 042331 (2003).

10. S. Gasel, N. Gisin, G. Ribordy, and H. Zbinden, "Quantum key distribution over 30km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods", *European Physical Journal D* **30**, 143--148 (2004).

11. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin "Quantum cryptography using entangled photons in energy-time Bell states", *Physical Review Letters* **84**, 4737--4740 (2000).

12. Id Quantique, "Single-photon detection with InGaAs/InP avalanche photodetectors", http://www.idquantique.com, (2005).

13. MagiQ Technologies, Inc., "MagiQ quantum cryptography test bed: uncompromising research results", *http://www.magiqtech.com*, (2005).

14. A. W. Davis, M. J. Pettitt, J. P. King, and S. Wright, "Phase Diversity Techniques for Coherent Optical Receivers", *Journal of Lightwave Technology* **5**, 561--572 (1987).

15. T. Okoshi and K. Kikuchi, *Coherent Optical Fiber Communications*, (KTK Scientific, 1988).

16. J. M. Kahn, "1Gbit/S PSK homodyne transmission system using phase-locked semiconductor lasers", *IEEE Photonics Technology Letters* **1**, 340--342 (1989).

17. J. M. Kahn, “BPSK homodyne detection experiment using balanced optical phase-locked loop with quantized feedback”, *IEEE Photonics Technology Letters* **2**, 1041--1135 (1990).

18. J. M. Kahn, A. H. Gnauck, J. J. Veselka, S. K. Korotky, and B. L. Kasper, “4-Gb/S PSK homodyne transmission system using phase-locked semiconductor lasers”, *IEEE Photonics Technology Letters* **2**, 285--287 (1990).

19. J. R. Barry, and E. A. Lee, “Performance of coherent optical receivers”, *Proceedings of the IEEE* **78**, 1369--1394 (1990).

20. J. R. Barry, and J. M. Kahn, “Carrier synchronization for homodyne and heterodyne detection of optical quadriphase-shift keying”, *Journal of Lightwave Technology* **10,** 1939--1951 (1992).

21. S. Betti, G. De Marchis, and E. Iannone, *Coherent Optical Communications Systems*, (Wiley 1995).

22. B. Glance, “Performance of homodyne detection of binary PSK optical signals”, *Journal of Lightwave Technology* **4**, 228--235 (1996).

23. P. J. Winzer, and H. Kim, “Degradation in balanced DPSK receivers”, *IEEE Photonics Technology Letters* **15**, 1282--1284 (2003).

24. K. P. Ho, “The effect of interferometer phase error on direct-detection DPSK and DQPSK Signals”, *IEEE Photonics Technology Letters* **6**, 308--310 (2004).

25. C. Xu, X. Liu, and X. Wei, “Differential phase-shift keying for high spectral efficiency optical transmissions”, Invited Paper *IEEE Journal of Selected Topics in Quantum Electronics* **10**, 281--293 (2004).

26. A. H. Gnauck, and P. J. Winzer, “Optical phase-shift-keyed transmission”, *Journal of Lightwave Technology* **23**, 115--130 (2005).

27. K. P. Ho, *Phase-Modulated Optical Communication Systems*, (Springer 1st edition, 2005).

CHAPTER 2 QUANTUM CRYPTOGRAPHY

2.1 HISTORY OF THE CRYPTOGRAPHY AND CRYPTANALYSIS

Back to the ancient Greece and Rome time for at least two thousand years there have been people who wanted to send messages that could only be read by the people for whom they were intended. When a message is sent from the sender to the recipient, whether by the slave or by the post office today, or by means of telegraph, radio, telephone, fax or e-mail, there is a risk of it going astray. If the message is written in clear, that is, in a natural language without any attempt at concealment, anyone getting hold of it will be able to read it and, if they know the language, understand it.

Before the modern era, cryptography was concerned solely with message confidentiality, i.e., encryption — conversion of messages from a comprehensible form into an incomprehensible one, and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge. Namely, the key is needed for decryption of that message.

The two world wars of the 20th century had accelerated the development of the new cryptographic techniques. In 1917, Gilbert S. Vernam proposed an unbreakable cryptosystem, hence called Vernam Cipher or One-time Pad (OTP) [1]. In the recent 30 to 40 years, with the explosive developing speed of the information technology the field has expanded beyond confidentiality concern to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, interactive proofs, and secure computation, amongst others.

We first define some of the key notions in the modern cryptography system.

A *cipher system,* or *cryptographic system*, or *crypto-system*, is any system that can be used to change the text of a message with the aim of making it unintelligible to anyone other than intended recipients.

The process of applying a cipher system to a message is called *encipherment* or *encryption*. The reverse process to encipherment, recovering the original text of a message from its enciphered version, is called *decipherment* or *decryption*.

Cryptography is the study of the design and use of cipher systems including their strengths, weaknesses and vulnerability to various methods of attack. A *cryptographer* is anyone who is involved in cryptography.

Cryptanalysis is the study of methods of solving cipher systems. A *cryptanalyst*, often popularly referred to as a code breaker, is anyone who is involved in cryptanalysis.

2.2 PUBLIC-KEY (ASYMMETRIC) CRYPTOGRAPHY

As we have discussed in 1.1, in the real world secure communications have to be established between two or more users who have never met before to share the secret cryptographic key. The question now is how to distribute the key to those users. In 1976 Whitfield Diffie and Martin E. Hellman have invented the public-key cryptography [2].

Public-key cryptography, also known as *asymmetric cryptography*, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

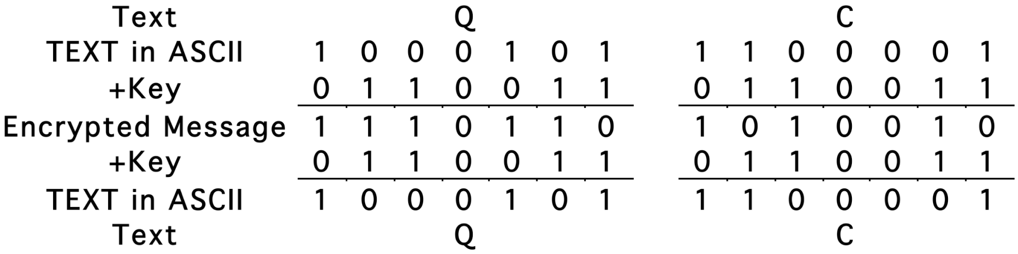
The security of public-key cryptography rests on the computational complexity like factoring the product of two large primes or computing discrete logarithms. However, no public-key encryption scheme can be secure against eavesdroppers with nearly unlimited computational power, except from quantum computer. Proofs of security therefore hold with respect to computationally limited adversaries, and give guarantees, i.e. relative to a particular mathematical assumption, of the form “the scheme cannot be broken using a desktop computer in 1000 years”.

Public-key cryptosystems are convenient and have thus become very popular over the last 25 years. The security of the Internet is partially based on such systems. For example, anyone can send an email to a mailbox, but only the legitimate one who holds thee password (as a private key) can read it.

2.3 PRIVATE-KEY (SYMMETRIC) CRYPTOGRAPHY

Private key cryptosystems require the use of a signal key for both encryption and decryption. These systems are believed to be safe as long as the OTP is used.

Alice encrypts her message, a string of binary bits denoted by *M*, by using a randomly generated key *K* of the same length. Each bit of *M* is added to the corresponding bit of *K* to obtained the scrambled text *S*: $S = (M \oplus K)\mathrm{mod}2$. The text *S* is then sent to Bob who then decrypts the message by subtracting the key and obtain $M' = (S \oplus K)\mathrm{mod}2 = M$. Since the key is a random series of bits, the scrambled message contains no information according the security proof of Shannon [3]. And this is the only provable secure cryptosystem known today.



Text				Q							C			
TEXT in ASCII	1	0	0	0	1	0	1	1	1	0	0	0	0	1
+Key	0	1	1	0	0	1	1	0	1	1	0	0	1	1
Encrypted Message	1	1	1	0	1	1	0	1	0	1	0	0	1	0
+Key	0	1	1	0	0	1	1	0	1	1	0	0	1	1
TEXT in ASCII	1	0	0	0	1	0	1	1	1	0	0	0	0	1
Text				Q							C			

Figure 2.1 Message encryption and decryption using the same key

Nevertheless, in a practical communications system, the key *K* can be only be used once, since the eavesdropper can store up all the messages and figure out the key and the messages, given the advances in technology and mathematical algorithms. Furthermore another fundamental problem of the private-key cryptosystems is that we cannot store an infinite number of different keys, therefore a constant key regeneration procedure is mandatory.

2.4 QUANTUM CRYPTOGRAPHY

As a matter of fact, within the framework of classical physics, it is impossible to reveal potential eavesdropping, because information encoded into any property of a classical object can be acquired without affecting the state of the object. All classical signals can be monitored passively since one bit of information is encoded on two distinguishable states of hundreds of photons, electrons or other carriers.

2.4.1 QUANTUM MEASUREMENTS

However in quantum measurements it is possible to distinguish with certainty only among specific orthogonal state vectors. Here are some basic quantum mechanics theorems:

- It is impossible to measure the states of a quantum system without perturbation;
- It is impossible to determine simultaneously two different physical characteristics with an arbitrary precision;
- It is impossible to measure simultaneously a photon in two orthogonal bases without destruction;
- It is impossible to copy a photon without destroying it, the non-cloning theorem.

2.4.2 BB84 Protocol

Charles H. Bennett of IBM and Gilles Brassard of the University of Montreal proposed the first protocol for quantum cryptography (QC) in 1984, hence the name BB84 [3]. Generally, the quantum cryptography protocol concerns the term quantum key distribution (QKD), and it is the only subject of discussion here.

In these protocols [4], the two protagonists Alice and Bob use two channels of communications: one quantum channel of course, and another classical channel [5,6]. The quantum channel allows the transmission of quantum objects. The quantum objects have to be very weak so that quantum effects are measurable. The precise nature of the these objects depends on the concerned protocols, nevertheless in practice attenuated laser pulses are widely used, transit in optical fibers or in open space. The eavesdropper, namely Eve, is supposed to have access to this quantum channels even the quantum channel nature limits its actions.

In the other hand, the classical channel that permits Alice and Bob to communicate could be a telephone line, an Ethernet cable or even radio frequency. This channel is also supposed spied by Eve who listens to the conversation between Alice and Bob, but she would modifier the information in the channel. In other terms, this channel should be authenticated, which is possible by the classical cryptography algorithm, since Alice and Bob share *a priori* some secret key.

First of all Alice and Bob exchange the quantum objects through the quantum channel. These objects are prepared in such a way that Eve's tentative of acquiring the information will induce, in accordance with the quantum mechanics, by a perturbation of the signals that Alice and Bob could measure by comparing the communications through the classical channel.

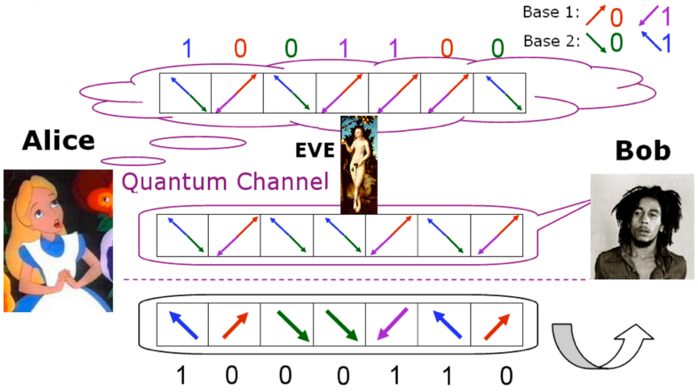


Figure 2.2 BB84 in quantum channel

1 - Alice chooses a random series of bits;

2 - Alice sends each bit with a random base choice (base 1 or base 2);

3 - Bob detects each bit using another random choice of the base (base 1 or base 2).

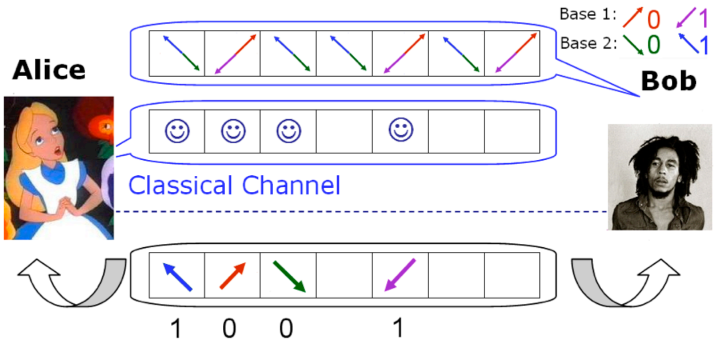


Figure 2.3 BB84 in classical channel

4 - Bob publicly announces his series of base choices (not the measurement results!);

5 - Alice publicly announces the base coincidences i.e. the bits correctly detected by Bob;

6 - Bob and Alice use this bit sequence as the key, a raw key is thus generated.

When there is base coincidence, i.e., Bob and Alice chose the same base, the bit is correctly detected and when there is base anti-coincidence, the measurement result is random. The sequence obtained when there are base coincidences is kept, and then some of these bits are chosen to perform the eavesdropping test, i.e. privacy amplification. Alice and Bob compare these symbols of raw keys to obtain a sifted key, which is then used for the encryption of the message.

As a matter of fact, in the quantum channel, Bob's raw bit error rate (BER) is 0.25 since the base coincidence and base anti-coincidence are equal-probable, and half of the anti-coincidence bits will be wrongly detected. After the communications in the classical channel and the "reconciliation" process, the theoretical post-detection BER should be 0 since bits of anti-coincidence are abandoned.

As a matter of fact, the raw BER and post-detection BER will change under Eve's attack, but these BER variations can also be induced by the channel imperfections that add noise to the signal. Consequently any virtual noise should be considered as Eve's intervention as Eve is assumed capable of hiding her presence under such a noise level, even though some of the noise is, in fact, induced by experimental imperfections or system impairments. Alice and Bob can effectively measure the perturbations and thus evaluate the quantity of information gained by Eve. If Eve's information gain is lower than that of Bob's, the procedure of "Privacy Amplification" can be used to extract a secret key, rending Eve's intervention (attacks) irrelevant [7,8]. On the other hand, if Alice and Bob acknowledge that Eve has gained more information than Bob from her intervention, then they will simply abandon the generated keys, or eventually counter-attack by giving false information.

2.4.3 POLARIZATION ENCODING

Thanks to the commercially available polarization beam splitter, polarization encoding on photons appeared to be the first natural solution for QKD system. Bennett and his co-workers (Bennett, Bessette, *et al.* 1992) had done the first experimental demonstration of a QKD system [9]. They have implemented a system in which Alice and Bob exchanged faint light pulses produced by a light diode and containing less than 1 photon on average over a distance of 30 cm in air. This small-scale experiment has since invoked great research interests since it showed that it was not unreasonable to use single photons as information carrier, instead of classical pulses for encoding bits.

In a typical QKD system using the BB84 four-state protocol, Alice emits short classical photon pulses polarized at -45°, 0°, 45°, and 90° by four laser diodes. For one given qubit, one single diode is triggered. The pulses are then attenuated by a set of attenuators to reduce the average number of photons to well below 1, and sent along the quantum channel to Bob. At Bob's side, the transmitted photons are analyzed in the vertical-horizontal bases with a polarizing beam splitter and two photon-counting detectors.

It is essential to maintain the polarization states of the emitted pulses so that Bob would be able to extract the information encoded by Alice. As the polarization state is arbitrarily transformed in the standard optical fiber, it is necessary for a real fiber-based QKD system to actively align the polarizations to compensation for this evolution. Although this procedure is not impossible, the tasks are very difficult, especially for practical long distance applications. One possible solution has been considered by using polarization-maintaining fibers. Although the birefringence of the so called polarization-maintaining (PM) fiber is large enough to effectively uncouple the two polarization eigen-modes, only these two orthogonal polarization modes are maintained, consequently these fibers cannot maintain all the required polarization states. All the other modes, in contrast, evolve very quickly, making this kind of fiber completely unsuitable for polarization based QKD system. As we will mention later, PM fibers can be used in phase-based QKD system, since only one of the two orthogonal polarizations states are needed.

2.4.4 Phase Encoding and Frequency Encoding

Bennett first proposed phase encoding method for QKD system in 1992, for the two-state protocol, namely BB92 [10], it is indeed a natural choice for optics scientists and researchers. Phase encoding protocol can be realized with interferometers in single mode fiber components. A typical system consists of a double Mach-Zehnder (MZ) implementation, as shown in Figure 2.4: a MZ interferometer at Alice's end and another MZ interferometer at Bob's end. The interferometers are made of symmetric couplers or beam splitters.

At Alice's side the lightwave pulses are generated by a pulsed laser and then separated by an optical coupler. The lower arm signal is phase-modulated to generate a four-state QPSK constellation, and the phase shift for a given qubit is Φ_A. The signal is then time-multiplexed with the local oscillator (LO), i.e., the upper arm component before entering in the propagation channel that is consisted of single mode optical fiber. At the receiver Bob's end, the LO pulse goes through a phase shift Φ_B before beating with the signal pulse that carries a phase shift Φ_A.

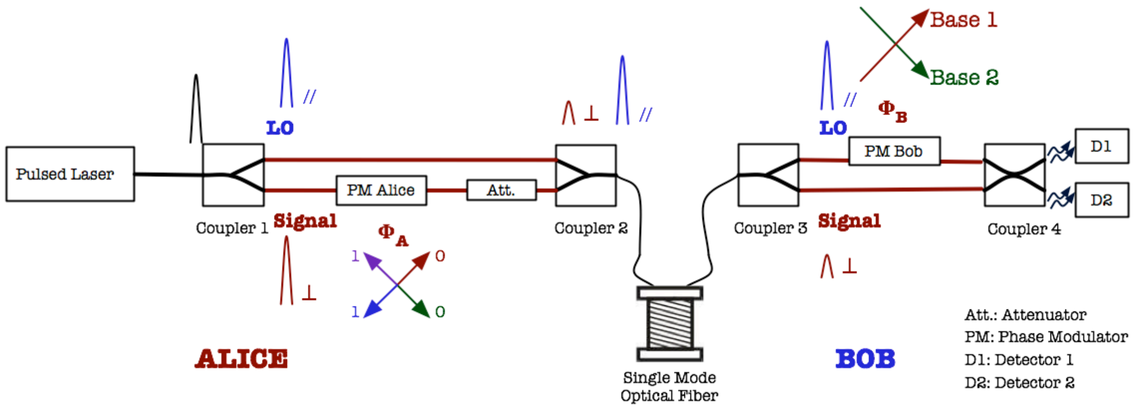


Figure 2.4 Double Mach-Zehnder QKD system implementation

Provided that the coherence length of the light used is larger than the path mismatch in the interferometers, interference fringes can be recorded. When single photon counters are used as D1 and D2, we will detect one click at D1 when $\Phi_A - \Phi_B = 0$, or one click at D2 when $\Phi_A - \Phi_B = \pi$, actually these two cases correspond to the base coincidence situation. When $\Phi_A - \Phi_B = \pm\pi/2$, the photon arrives at D1 or D2 in a random way, and these two cases correspond to the base anti-coincidences.

It is mandatory with this scheme to keep the path difference stable during a key exchange session, since a drift of the length of one arm would indeed change the phase relation between Alice and Bob and induce errors in their bit sequence. A "plug-and play" scheme has been proposed by Muller and Zbinden's research group in 1997 [11,12] to compensate the phase fluctuations of the QKD system automatically. Two Faraday mirrors – a mirror with a λ/4 Faraday rotator in front, are used in the system to compensate automatically the polarization variations in the propagation, as well as to compensate the path difference since the signal pulse and the LO pulse propagate in the same physical optical path. However this scheme requires that the laser source to be placed at Bob's end and double the transmission distance. Also in this scheme, the pulses are more than a thousand times brighter before than after reflection from Alice. Backscattered photons can accompany a quantum pulse propagating back to Bob and induce false counts. One will have to make sure that the pulses traveling to and from Bob are not present in the lime simultaneously, however this requires reducing the effective repetition frequency. Moreover, the main disadvantage is with respect to the security issues, since they are more sensitive to Trojan house attacks.

Goedgebuer and Merolla's team from University of Besancon in France have introduced a "frequency encoding" scheme [13], using radio-frequency side band modulation at both Alice's and Bob's sides, and Bob can record the interference pattern in these sidebands after removals of the central frequency and the higher-order sidebands with a spectral filter. The advantage of this scheme is that the interference is controlled by the phase of the radio-frequency oscillators. However the detector noise is relatively high due to the long pulse durations, also the polarization transformation in an optical fiber depends on the wavelength that contributes to the imperfect interference visibility, also the error rate is higher than that measured with plug-and-play system. Moreover the phase modulator needs to be polarization independent and the stability of the frequency filter can be a practical difficulty.

Takesue, Diamanti and Yamamoto's groups from NTT and Stanford university [14,15] have implemented a differential phase shift quantum key distribution (DPS-QKD) protocol, which uses a Poisson light source and a detector for the 1.5 μm band frequency up-conversion in a periodically poled Lithium Niobate waveguide followed by an Si avalanche photodiode. This detector design takes advantages of good properties of near-infrared band single-photon detection and the DPS-QKD protocol has simplified the receiver structure, however the 10GHz PLC Mach-Zehnder interferometer still requires very precise thermal control.

Xiao-Fan Mo *et al*. [16] has implemented a unidirectional intrinsically stable QKD scheme that is based on Michelson–Faraday interferometers, in which ordinary mirrors are replaced with 90° Faraday mirrors to compensate automatically the phase and polarization variation. With the scheme, a demonstration setup was built and good stability of interference fringe visibility was achieved over a fiber length of 175 km.

Hirano [17] has implemented an experimental 1.5 μm QKD system that utilizes pulsed homodyne detection, instead of photon counting, to detect weak pulses of coherent light. Although the scheme inherently has a finite error rate, homodyne detection allows high-efficiency detection and quantum state measurement of the transmitted light using only conventional devices at room temperature. The quantum channel is a 1-km standard optical fiber and the probability distribution of the measured electric-field amplitude has a Gaussian shape. The effect of experimental imperfections such as optical loss and detector noise limit the system performance, as well the long-term phase drift should be compensated for a practical operation.

REFERENCES

1. G. Vernam, “Ciper printing telegraphe systems for secret wire and radio telegraphic communications”, *Journal American Institute of Electrical Engineering* **55**, 109--113 (1926).
2. W. Diffie, and M. E. Hellman, “New directions in cryptography”, *IEEE Transactions on Information Theory* **22**, 644--654 (1976).
3. C. E. Shannon, “A mathematical theory of communication”, *Bell System Technical Journal* **27**, 379--423 & 623--656 (1948).
4. C. H. Bennett, and G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, *Proceeding of IEEE International Conference on Computers, systems, and Signals Processing*, 175-179 (1984).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, *Reviews of Modern Physics* **74**, 145--195 (2002).
6. T. P. Spiller, “Quantum information processing: cryptography, computation, ant teleportation”, *Proceedings of the IEEE* **84**, 1719--1746 (1996).
7. J.-P. Marc, G. Brassard, and C. H. Bennett, “How to decrease your enemy's information”, *Advances in Cryptology: Proceeding of Crypto* **85**, H. C. Williams ed., Lecture Notes in Computer Science **218**, 468--476 (Springer Berlin 1986).
8. C. H. Bennett, G. Brassard, and J.-M. Robert “Privacy amplification by public discussion”, *S.I.A.M. Journal on Computing* **17**, 210--229 (1988).

9. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography”, *Journal of Cryptology* **5**, 3--28 (1992).

10. C. H. Bennett, “Quantum cryptography using any two nonorthogonal states”, *Physical Review Letters* **68**, 3121--3124 (1992).

11. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “Plug and play’ systems for quantum cryptography”, *Applied Physical Letters* **70**, 793--795 (1997).

12. H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, “Interferometry with Faraday mirrors for quantum cryptography”, *Electronics Letters* **33**, 586--588 (1997).

13. J.-M. Mérolla, Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, , “Single-photon interference in sidebands of phase-modulated light for quantum cryptography”, *Physical Review Letters* **82**, 1656--1659 (1999).

14. H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, “Differential phase shift quantum key distribution experiment over 105-km fiber”, *New J. Phys.* **7**, 232 (2005), e-print arXiv:quant-ph/0507110.

15. E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, “100 km differential phase shift quantum key distribution experiment with low-jitter up-conversion detectors”, *Opt. Express* **14**, 13073 (2006), e-print arXiv:quant-ph/0608110.

16. X.-F. Mo, B.Zhu, Z.-F. Han, Y.-Zh. Gui, and G.-C. Guo, “Faraday-Michelson system for quantum cryptography”, *Opt. Lett.* **2632** (2005).

17. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection”, *Physical Review A* **68**, 042331 (2003).

CHAPTER 3 CHALLENGES IN EXPERIMENTAL QUANTUM KEY DISTRIBUTION SYSTEMS

The inventors of the protocol BB84 Charles H. Bennett and Gilles Brassard originally proposed using photon polarization states to transmit the information. The very first experimental demonstration was performed in IBM laboratory as an open space link over a distance of 32 cm at the wavelength of 550 nm [1]. In order to have a practical interest, a QKD system should be designed to establish a secured link of at least several kilometers and compatible with the current infrastructures. Over the latest years, most research groups are seeking for a reliable high speed and long distance fiber-optic QKD systems.

3.1 SINGLE PHOTON SOURCES

As mentioned in the chapter 2, the quantum cryptography is based on the quantum mechanics theorems and, basically by the use of single-photon Fock states $|n\rangle$, i.e. any state having a well-defined number of particles, since Eve can easily steal one photon in a state of multi-photon.

The only idea of single photon source is that the source should emit exactly one photon in response to a trigger pulse, which can be either electrical or optical. The operating principle is shown in Figure 3.1. The source consists of a single emissive element, i.e. an atom, and the trigger pulse excites the atom to an upper excited state. The atom then emits a cascade of photons as it relaxes to the ground state. Since the photons have different wavelengths, it is possible to select the photon from a particular transition by filtering the fluorescence. There will only be one photon emitted from a specific transition in each cascade.

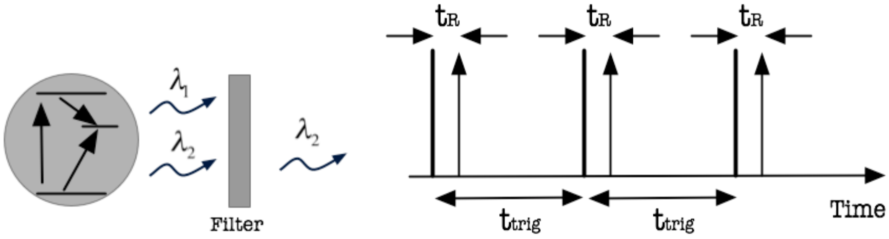


Figure 3.1 Excitation-emission cycles from a single atom in response to trigger pulses.

(a) The atom emits a cascade of photons of different wavelengths as it relaxes, but by using a suitable filter, only one of them is selected. (b) Schematic representation of the photon emission sequence.

As intense trigger pulse rapidly promotes an electron to the excited state, the atom will emit exactly one photon after a time roughly equal to the radiative lifetime t_R, as show in Figure 3.1 (b). No more photons can be emitted until the next trigger pulse arrives, when the process repeats itself. The time separation of the trigger pulses is determined by the frequency f_{trig} at which the trigger source operates. If the time separation $t_{trig} = 1/\ f_{trig}$ between the pulses is significantly longer than t_R, then the trigger pulses control the separation of the photons in the fluorescence. We thus have a source that emits exactly one photon of a particular wavelength whenever a trigger pulse is applied.

Experiments describing a molecular single-photon source are reported by Lounis and Moerner [2], an equivalent experiments for color centers in diamond are described by Kurtsiefer [3]. The first two results on quantum dot single-photon sources have also been described by Michler [4] and Santori [5], as well all of these experiments are optical trigger pulses. Z. Yuan has reported an electrically driven single-photon source [6].

3.2 ATTENUATED POISSONIAN LASER SOURCE

Up to today the technologies of single photon sources are not mature enough to be commercialized, thus most research groups rely on fainted laser pulses to generate weak coherent states [7] or entangled photon pairs, in which the photon-number distribution follows Poisson statistics.

Poisson statistics generally apply to random processes that can only return integer values. The average count value $\bar{n}$ is determined by the half-life of the laser source, the amount of material present, and the time interval set by the user. The actual count values fluctuate above and below the mean value due to the random nature of the radioactive decay. Given the average photon number of a coherent state $\bar{n}$, the probability of obtaining n photon in a fainted pulse is:

$$P\left(n,\bar{n}\right)=\frac{\bar{n}^{n}}{n!}e^{-\bar{n}} \tag{3.1}$$

Poisson distributions are only characterized by their mean value $\bar{n}$ since the fluctuations of a statistical distribution about its mean value are usually quantified in terms of the variance. The variance is equal to the square of the standard deviation Δn that is defined as:

$$Var(n)\equiv(\Delta n)^{2}=\sum_{n=0}^{\infty}\left(n-\bar{n}\right)^{2}P(n)=\bar{n} \tag{3.2}$$

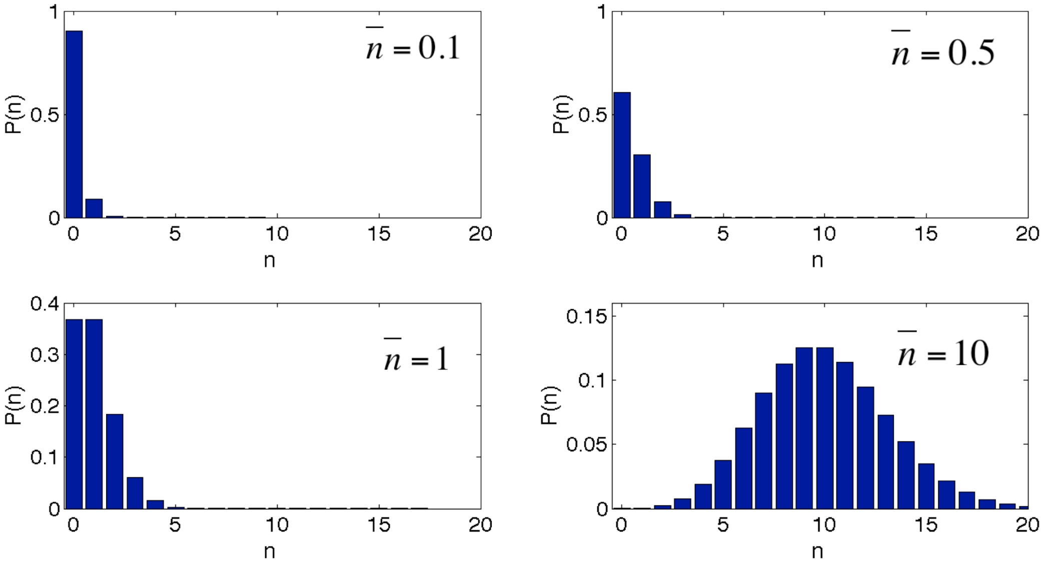


Figure 3.2 Poisson distribution for mean photon number values of 0.1, 0.5, 1.0, and 10

It is to be noted that in Figure 3.2 the vertical axis scale changes in each figure. The standard deviation for the fluctuations of the photon number above and below the mean value is therefore given by:

$$(\Delta n) = \sqrt{\bar{n}} \tag{3.3}$$

Those coherent states that contain more than one photon are considered non-secure:

$$P\left(n > 1 \mid n > 0, \bar{n}\right) = \frac{1 - P\left(0, \bar{n}\right) - P\left(1, \bar{n}\right)}{1 - P\left(0, \bar{n}\right)} \tag{3.4}$$

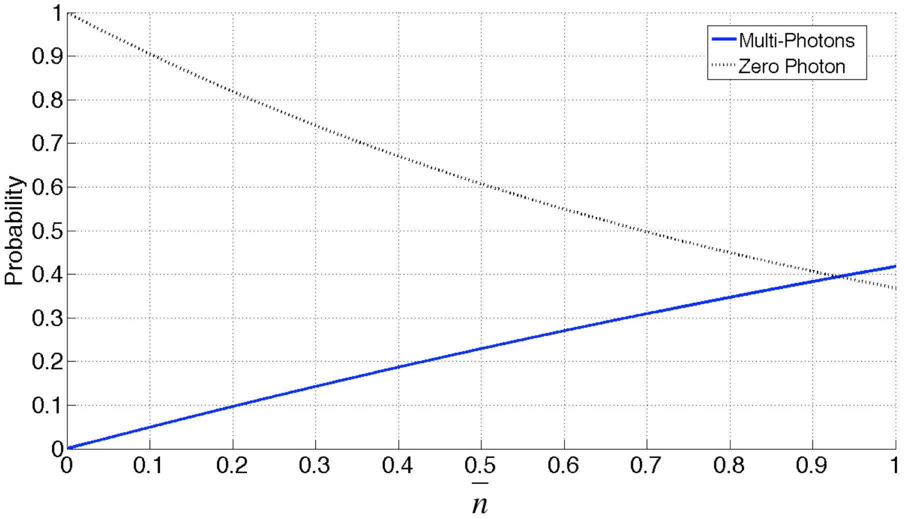


Figure 3.3 Probability of multi-photons pulse and zero-photon pulses

We can make the multi-photon pulse probability arbitrarily small by chosing a very small $\bar{n}$. However, the drawback is that in this case most pulses are of zero-photon, the trade-off for the security is a reduction in the quantum key generation rate. Most experiments have adapted to use in the range around 0.1, meaning that 5% of the nonempty pulses contain more than one photon. Nevertheless, the optimal value depends on the transmission losses, e.g. at 1550 nm the fiber loss is around 0.2 dB/km and the dispersion parameter is about 17 ps/km nm.

3.3 QUANTUM CHANNEL IMPAIRMENTS

The quantum channel is the link between the sender Alice and the receiver Bob that transmit the quantum objects. Physically speaking, the quantum channel is not different from the classical channel, they can be either free-space link or optical fiber; the main difference lies in the fact that in quantum channel the information is encoded on single photon while in a classical channel many photons carry the same information. From this point of view, all the classical channel impairments will be inherited by the quantum channel, such as optical fiber attenuation due to material absorption, Rayleigh scattering, chromatic dispersion and polarization mode dispersion (PMD), as well as other non-linear effects in silica fibers.

Free-space quantum channel offers some advantages for establishing a quantum channel. The atmosphere has a high transmission window at wavelength around 700 nm where commercial high quantum efficiency photon detection modules are available. Moreover, this media is weakly dispersive and the non-birefringent. The first experimental demonstration of a QKD system was performed in a free space link [8,9]. However, there are also some drawbacks that limit it from being a more practical technical choice: it suffers from a high and variable transmission loss; the beam divergence that caused by diffraction at the transmitter aperture increases with the transmission distance. Furthermore an open link offers an easy access to the eavesdropper Eve.

Nowadays most research groups are using telecom wavelength single mode fibers [10-15] as the quantum channel, for its low losses in a “protected” propagation, e.g. optical fibers, and the compatibility with the installed infrastructure. On the other hand, the polarization effects due to the birefringence – the two different phase velocities for two orthogonal polarization states that are caused by the asymmetric fiber internal structure, become a main impairment. This phenomenon can be counteracted by polarization-maintaining optical fiber because the birefringence is large enough to effectively uncouple the two polarization eigenmodes. But only the two orthogonal polarization states are maintained, all other modes evolve very quickly, thus making it an unsuitable choice for polarization encoding QKD system.

Phase encoding is thus a better choice in an optical fiber based system [12,13]. Using two similar Mach-Zehnder interferometers, Alice encodes the information on the weak light pulse at her end, and Bob performs his base choice before the signal detection. Unfortunately due the nature of Mach-Zehnder interferometer, even slightly mechanical vibrations and slow temperature variations can induce the mismatch between the optical paths in the two arms, thus leading to an inevitable phase drift even if the interferometers are well placed in styrofoam boxes or under precise temperature control. Therefore an active feedback to track and compensate the phase-errors is necessary for a practical communications system. A "plug and play" two-way system has also been proposed and investigated to combat with the polarization and phase drift issues [14-17].

3.4 SINGLE PHOTON DETECTION

Photodiodes are semiconductor devices designed to transform light into an electric current and are used as detectors in numerous applications. The simplest photodiode is the so-called PIN junction diode, which operates at zero or low reverse bias and provides no internal current gain. Although PIN. diodes can be used for sensitive detection when followed by a low-noise electrical amplifier, they feature too much noise for detecting single photons. An avalanche photodiode (APD) is basically a PIN diode specifically designed for providing an internal current gain mechanism. When reverse biased, the APD is able to sustain a large electric field across the junction. An incoming photon is absorbed to create an electron-hole pair. The charge carriers are then swept through the junction and accelerated by the strong electric field. They can gain enough energy to generate secondary electron hole pairs by impact ionization. These pairs are in turn accelerated and can generate new electron-hole pairs. This multiplication phenomenon is known as an avalanche.

As the most critical part of the success of a quantum cryptography system is the single photon detection, the single photon detection module (SPDM) should not only detect the photon and record the information that it carries, but also operates under an almost noise-free condition to minimize the false detection events. One of the choices today is the APDs that operate in the Geiger-mode. We also call it single photon avalanche diode (SPAD).

SPAD, exploiting the photon-triggered avalanche current of a reverse biased p-n junction to detect an incident radiation, is specifically designed to operate with a reverse bias voltage well above the breakdown voltage [18,19]. An incoming photon will generate an electron avalanche consisting of thousands of carriers. Te reset the diode, a quenching process is a must to stop the emissions and recharge the diode. Gated-mode operation is often used to keep the bias voltage below the breakdown voltage and raise it above only for several nanoseconds when a photon is expected to arrive. SPAD is thus commonly used in the quantum cryptography based on fainted laser pulses with synchronized clock signals.

Figure 3.4 represents the I-V characteristics of an APD and illustrates how single-photon sensitivity can be achieved. This mode is also known as Geiger mode. The APD is biased, with an excess bias voltage, above the breakdown value and is in a metastable state (point A). It remains in this state until a primary charge carrier is created. In this case, the amplification effectively becomes infinite, and even a single-photon absorption causes an avalanche resulting in a macroscopic current pulse (point A to B), which can readily be detected by appropriate electronic circuitry. This circuitry must also limit the value of the current flowing through the device to prevent its destruction and quench the avalanche to reset the device (point B to C). After a certain recovery time, the excess bias voltage is restored (point C to A) and the APD is again ready to detect a photon.

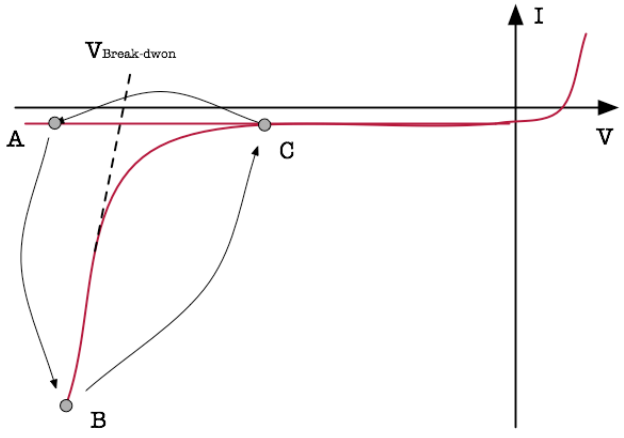


Figure 3.4 I-V characteristics of single photon detection

Some operating effects of SPAD are that the "counting events" can not only be generated by the information carrier, but also by the unwanted impinging photons or without any photon at all, i.e. the dark counts. Dark counts are induced by thermal or band-to-band tunneling process, etc. The afterpluses are spurious counts caused by carriers trapped in deep levels introduced by impurities of crystal defects, and those that are released within a subsequent gate also add to the "false counts". In fact, the number of trapped charges decreases exponentially with time. So the tradeoff of having less afterpluses induced "false counts" is to apply a longer "dead time", i.e. the interval between two consecutive gate operations. The exponential time constant decrease of afterpulses could shorten the "quenching process" when operating under a higher temperature, however at the same time it will generate more thermal noise too.

Effectively the tradeoff is to be found in the operation parameters: bias voltage, temperature, and the dead time that limits the operational frequency. For example, at the telecom wavelength 1550 nm, InGaAs APD operates at 173 K and has a dark count rate of 10^{-4} counts/s, with quantum efficiency in the range of 10%.

The detection efficiency η can be obtained using the following formula:

$$\eta = \frac{1}{n}\ln\frac{p_{dc}-1}{p_{dc}+p_{sig}-1} \qquad (3.5)$$

where η is the quantum detection efficiency, n is average photon number per pulse, p_{dc} is the dark count probability per gate, and p_{sig} is the signal count probability per gate. With a higher average photon number n, we will evidently have a higher p_{sig}. However, the probability of receiving multi-photon pulse at a gate operation increases when the average photon number n is higher, as we have already shown in Figure 3.2 and Figure 3.3, since the cooled APD cannot distinguish the single and multiple photons pulses. Therefore when using weak Poissonian light pulses, the detection efficiency will be closer to the real quantum efficiency of the gated APD, and will decrease when n increases.

Recently Toshiba Research Europe has proposed a photon-number-resolving APD detector configuration [20] to measure the very weak avalanches at the early stage of their development. They split the output signal from the APD into two paths – one of which introduces a delay of one period of the alternating bias voltage relative to the other path. The periodic capacitive response signal from the APD is thus virtually eliminated by taking the difference between the signals in the two paths. They reported an operational frequency at 622 MHz with negligible dark count (< 2×10^{-6} per gate) and claimed that this receiver configuration is capable of discriminating the impinging mean photon number by observing the peak output signal statistics, which is proportional to the incident flux.

REFERENCES

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography”, *Journal of Cryptology* **5**, 3--28 (1992). Preliminary version

in *Advances in Cryptology - Eurocrypt '90 Proceedings*, 253--265 (Springer - Verlag 1990).

2. B. Lounis, and W. E. Moerner, “Single photons on demand from a single molecule at room temperature”, *Nature* **407**, 491-493 (2000).
3. C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, “Stable solid-state source of single photons”, *Physical Review Letters* **85**, 290--293 (2000).
4. P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, “A quantum dot single-photon turnstile device”, *Science* **290**, 2282--2285 (2000)
5. C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, “Triggered single photons from a quantum Dot”, *Physical Review Letters* **86**, 1502--1505 (2001).
6. Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, “Electrically driven single-photon source”, *Science* **295**, 102--105 (2002).
7. R. J. Glauber, “Coherent and incoherent states of the radiation field”, *Physical Review* **131**, 2766--2788 (1963).
8. B. Jacobs, and J. D. Franson, “Quantum cryptography in free space”, *Optics Letters* **21**, 1854--1856 (1996).
9. J. D. Franson, and H. Ives, “Quantum cryptography using optical fibers”, *Applied Optics* **33**, 2949--2954 (1994)

10. P. Townsend, “Experimental investigation of the performance limits for first telecommunications window quantum cryptography systems”, *IEEE Photonics Technology Letters* **10**, 1048--1050 (1998).

11. R. J. Hughes, G. L. Morgan, and C. Glen “Quantum key distribution over a 48 km optical fibre network”, *Journal of Modern Optics* **47**, 533--547 (2000).

12. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, *Reviews of Modern Physics* **74**, 145--195 (2002).

13. M. Martinelli, “A universal compensator for polarization changes induced by birefringence on a retracing beam”, *Optical Communications* **72**, 341--344 (1989).

14. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “‘Plug and play’ systems for quantum cryptography”, *Applied Physics Letters* **70**, 793--795 (1997).

15. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, “Automated ‘plug & play’ quantum key distribution”, *Electronic Letters* **34**, 2116--2117 (1998).

16. M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, “Experiments on long-wavelength (1550 nm) ‘plug and play’ quantum cryptography systems”, *Optics Express* **4**, 383--387 (1999).

17. H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, “Interferometry with Faraday mirrors for quantum cryptography”, *Electronics Letters* **33**, 586--588 (1998).

18. Id Quantique, “Single-photon detection with InGaAs/InP avalanche photodetectors”, http://www.idquantique.com, (2005).

19. MagiQ Technologies, Inc., “MagiQ quantum cryptography test bed: uncompromising research results”, *http://www.magiqtech.com*, (2005).

20. B. E. Kardynal, Z. L. Yuan, and A. J. Shields, “An avalanche-photodiode-based photon-number-resolving detector”, *Nature Photonics* **2**, 425--428 (2008).

CHAPTER 4 COHERENT OPTICAL DETECTION AND QUANTUM NOISE

4.1 HISTORICAL REVIEW OF OPTICAL FIBER COMMUNICATIONS

The optical fiber has been first proposed by Kao and Hockham (1966) [1] to guide light for information transmission, today it is the preferred medium for high-throughput point-to-point digital communication, due to its large bandwidth, low attenuation, immunity to interference, and high security. There has been historically four generations of fiber-optic transmission system [2,3].

The first generation, deployed in the 1970's, use multimode fibers at wavelength near 850 nm, suffered from three main limitations: *attenuation*, *chromatic dispersion*, and *modal dispersion*. The *attenuation* that limits the transmission between the transmitter and the receiver was about 2 dB/km. The dispersion of fiber limits the speed at which date can be transmitted since it cause short rectangle pulses to spread temporally into wider and smoother pulses as they propagate in the optical fiber. *Chromatic dispersion* occurs when light of different wavelength travels with different speeds since the phase velocity, v, of a wave in a given uniform medium is given by $v = c/n(f)$, where c is the speed of light in a vacuum and $n(f)$ is the refractive index of the medium that is a function of the frequency f of the light. Similarly, *multimode dispersion* occurs when different propagation modes of light with different speed exist in a multimode fiber.

The second generation of optic-fiber system was introduced in the 1980's, operated at 1300 nm to avoid chromatic dispersion, the wavelength of minimum chromatic dispersion in fiber. However it still used multimode fiber that suffers from multimode dispersion.

The third generation system was introduced in mid-1980's, using single mode fiber (SMF) at 1300 nm. The core radius of SMF is made much smaller so that only the single mode can propagate, thus the mode dispersion has been avoided, and however the attenuation of 0.5 dB/km was still not satisfactory.

In the search for long distance transmission, and to exploit the minimum attenuation optical fiber band between 1450 nm to 1650 nm, the fourth generation systems has been proposed in late-1980's. Most of today's commercially available optical fiber has a loss about 0.2 dB/km at the low-loss window around 1550 nm in which optical signal can be transmitted without regeneration. The limitation for such a system is the significant amount of chromatic dispersion, so only spectrally pure lasers with narrow linewidth single longitudinal mode can be used.

Erbium-doped fiber amplifiers (EDFA) that provide gain at the low-loss window around 1550 nm is often used to periodically amplify an optical signal to compensate for fiber loss over long distance. This low-loss window of optical fiber can accommodate many channels for dense wavelength-division-multiplexed (WDM) systems. EDFA can amplify many WDM channels together without crosstalk and distortion while adding some noise to the signal.

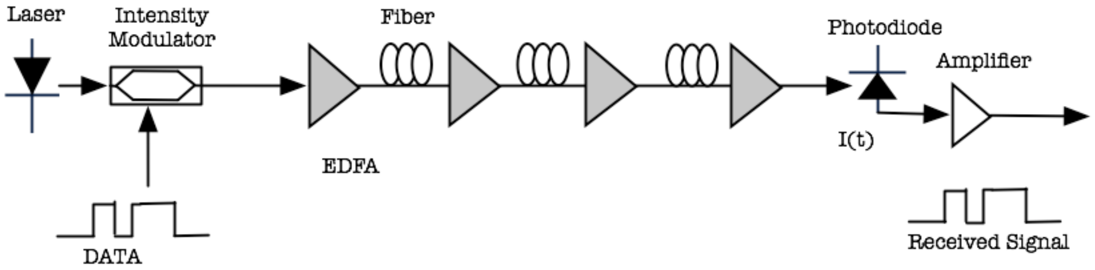


Figure 4.1 Typical configuration of an intensity-modulated/direct-detection system

In all commercialized optical communication systems, only the intensity of the optical signal is used to carry information, constituting a so-called on-off keying (OOK) or intensity-modulation/direct-detection (IM/DD) system. Intensity modulation refers the information is encoded only by the intensity of the transmitted light-wave, not on its frequency or phase. Direct detection means to the receiver configuration, in which the received signal is applied directly to a photo-detector. A practical optical receiver's sensitivity is measured by number of detected photon per bit to achieve a bit-error-rate (BER) of 10^{-9}. IM/DD systems, although easy to implement owning to its simple configuration, require 400 to 5000 photons per bit for such sensibility.

4.2 QUANTUM LIMIT FOR ON-OFF-KEYING

Light is a form of electromagnetic radiation, and can be represented by its electric or magnetic field. If the optical power is P_S, during a bit interval T, the average received photon per bit is:

$$\bar{n} = \frac{P_S T}{hv} \tag{4.1}$$

where v is the frequency (for wavelength $\lambda = 1550\ nm$, $v = 1.936 \times 10^{14}\ Hz$), h is the Planck's constant ($6.626 \times 10^{-34}\ \mathrm{J \cdot s}$).

Now we consider an ideal OOK transmission system over ideal channel in which the transmitter sends a pulse of light for bit "one" and no light for bit "zero". If a "zero" is transmitted, the probability of receiving any photon is 0. If a "one" is transmitted, as we have mentioned in the precedent chapter, the probability of obtaining n photon when the average photon number per bit is $\bar{n}$ follows Poisson statistics. And the BER can be induced only by receiving 0 photon when "one" is transmitted.

$$\begin{cases} \Pr\left[n > 0 \mid zero\right] = 0 \\ \Pr\left[n = 0 \mid one\right] = \dfrac{\overline{n}^{-n}}{n!} e^{-\bar{n}} = e^{-\bar{n}} \end{cases} \tag{4.2}$$

If we assume that "one" and "zero" are equally probable, then

$$BER = \frac{1}{2}\Pr\left[n > 0 \mid zero\right] + \frac{1}{2}\Pr\left[n = 0 \mid one\right] = \frac{1}{2}e^{-\bar{n}} \tag{4.3}$$

This leads to the lower bound on the BER called quantum limit [2-4]. The equation (4.3) gives a minimum signal power required to achieve a given BER. For example, to reach a BER = 10^{-9}, it sets a lower bound at $\bar{n} = 20$.

4.3 NOISE IN PHOTODETECTION

There are two main categories of noise: shot noise and thermal noise.

4.3.1 SHOT NOISE

The standard method used to detect light-wave is to employ photodiode detectors. Photodiode detectors are semiconductor devices that generate electrons in an external circuit when photons excite electrons from the valence band to the conduction band. A key parameter of the photodiode is *quantum efficiency* η, which is defined as the ratio of then number of photoelectrons generated in the external circuit to the number of photons incident. Given an optical power equal to P_S, the generated photocurrent is: $I = \eta e \frac{P_S}{hv}$. The ratio of $I/P = \frac{\eta e}{hv}$ is also defined as *responsivity* of the photodiode and has the unity A/W.

Shot noise is actually induced by Poisson process of the light-wave source, since the photocurrent generated by the beam fluctuates as a consequence of the underlying fluctuations in the impinging photon number. These photon number fluctuations will be reflected in the electron number fluctuations with a fidelity determined by η. If the average photocurrent number per bit $\bar{N}$ is generated by average impinging photon number per bit $\bar{n}$, then we have

$$\bar{N} = \eta \bar{n} \tag{4.4}$$

Then the variance of electron number $(\Delta N)^2$ and the variance of photon number $(\Delta n)^2$ have the relationship [5]:

$$(\Delta N)^2 = \eta^2 (\Delta n)^2 + \eta(1-\eta)\overline{n} \tag{4.5}$$

We can draw several very important conclusions from equation (4.5)

1. If $\eta = 1$, we have $\Delta N = \Delta n$ and electron number fluctuations reproduce the fluctuations of the incident photon stream.

2. As the incident photon stream has Poissonian statistics with $(\Delta n)^2 = \overline{n}$, then $(\Delta N)^2 = \eta \overline{n} = \overline{N}$ for any value η, thus the electron number also has a Poisson statistics.

3. If $\eta << 1$, the electron number fluctuations tend to has a Poisson statistics, but irrespective of the impinging photon statistics.

Therefore a high quantum efficiency photo-detector is necessary to reproduce faithful statistics of the impinging photocurrent.

Dark current I_{dark} has also to be taken into account when the impinging lightwave is weak, it is the constant response exhibited by a receiver of radiation regardless of the presence or the absence of incident photons. As a result, the current fluctuations have a standard deviation of

$$\begin{cases} \sigma_{shot}{}^2 = 2qI\Delta f \\ \sigma_{dark}{}^2 = 2qI_{dark}\Delta f \end{cases} \tag{4.6}$$

where q is the elementary charge of an electron, Δf is the bandwidth in Hz over which the noise is measured.

4.3.2 Thermal Noise

Thermal noise, also called Johnson–Nyquist noise, is the electronic noise generated by the thermal agitation of the charge carriers (usually the electrons) inside an electrical conductor at equilibrium, which happens regardless of any applied voltage. Thermal noise is approximately white, meaning that the power spectral density is equal throughout the frequency spectrum. Additionally, the amplitude of the noise has very nearly a Gaussian probability density function. The noise source can also be modeled by a current source in parallel with the resistor by taking the Norton equivalent that corresponds simply to a division by the impedance. This gives the root mean square value of the current source as:

$$\sigma_{thermal}{}^{2} = \frac{4k_B T}{R_{thermal}} \Delta f \tag{4.7}$$

where k_B is Boltzmann's constant (1.38×10^{-23} Joules/Kelvin), T is the resistor absolute temperature in Kelvins, and $R_{thermal}$ is the load resistor value in ohms, Δf is the bandwidth in Hertz over which the noise is measured.

Consequently, the photo-detector performance is dependent on the detection noise, i.e., shot noise and thermal noise:

$$\sigma^2 = \sigma_{shot}{}^{2} + \sigma_{dark}{}^{2} + \sigma_{thermal}{}^{2} = 2q\left(I + I_{dark}\right)\Delta f + \frac{4k_B T}{R_{thermal}} \Delta f \tag{4.8}$$

4.4 COHERENT RECEIVERS

Coherent optical transmission in telecommunications wavelength has been studied for more than three decades [6-10], due to its unique features concerning the use of complex amplitude modulations that allows lower optical signal-to-noise rate (OSNR) for a given post-detection BER. Coherent detection of optical signal is first used for its superior receiver sensitivity compared to OOK. The mixing of received signal field with the local oscillator (LO) laser functions as an optical amplifier without noise enhancement. Coherent detection can provide better receiver sensitivity even if EDFA is used in OOK. Furthermore, the use of the constant envelope formats, in opposition to the traditional intensity modulation with direct detection (IM/DD), is more tolerant to the non-linear effects in the fiber.

4.4.1 Single Branch Coherent Receiver

Coupler is defined physically as a passive optical device to two optical inputs and two outputs, whose role is to transmit signals input to output following a theoretical relationship called transfer function.

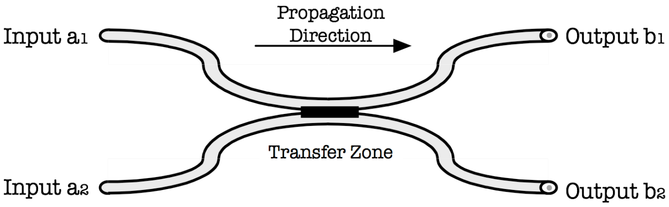


Figure 4.2 2×2 optical coupler

The basic principle is that the coupling between two evanescent wave fibers whose cores are very close. The electromagnetic field extending beyond the core, the light in one fiber core propagates gradually into the other through the transfer zone. These optical systems can be achieved by using the technique of polishing-assembly or fusion-stretching.

For a standard 50/50 optical 2×2 coupler in Figure 4.2, we can represent the electromagnetic fields transfer matrix of the inputs and outputs by:

$$C = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -j \\ -j & 1 \end{bmatrix} \tag{4.9}$$

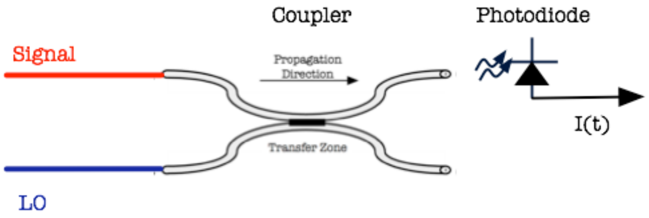


Figure 4.3 Single branch coherent receiver

Figure 4.3 shows a typical structure of single branch coherent receiver. To make an ideal and effective mixing, we make an assumption that the light can be represented by waves, and the polarizations of the two beams are perfectly matched. The signal field and the LO field can be represented by

$$E_{signal} = E_S e^{j(\omega_C t+\theta)} = \sqrt{P_S} e^{j\omega_0 t} e^{j(\omega_C t+\theta)} \tag{4.10}$$

$$E_{LO} = E_L = \sqrt{P_{LO}} e^{j\omega_0 t} \tag{4.11}$$

where ω_0 is the angular frequency of the lightwave, ω_C is the carrier angular frequency, and θ is the relative phase of the signal beam.

The optical power at the output of the coupler can be obtained:

$$\begin{aligned} P(t) &= \frac{1}{2}\left|E_{signal} + E_{LO}\right|^2 \\ &= \frac{1}{2}\left(P_S + P_{LO} + 2\sqrt{P_S P_{LO}}\cos(\omega_C t + \theta)\right) \end{aligned} \tag{4.12}$$

Therefore the photocurrent can be represented by

$$\begin{aligned} I(t) &= RP(t) + n_{shot}(t) + n_{thermal}(t) + n_x(t) \\ &= \frac{1}{2}R\left(P_S + P_{LO} + 2\sqrt{P_S P_{LO}}\cos(\omega_C t + \theta)\right) + n_{shot}(t) + n_{thermal}(t) + n_x(t) \end{aligned} \tag{4.13}$$

In equation (4.13), *R* is the responsivity of the photodiode and $n_{shot}(t)$ is the shot noise that is a zero mean process with power spectral density (PSD):

$$S_n(\omega) = qRP(t) \tag{4.14}$$

The thermal noise $n_{thermal}(t)$ is as mentioned in equation (4.7) with PSD:

$$S_{thermal}(\omega) = \frac{4k_B T}{R_{thermal}} \tag{4.15}$$

And $n_x(t)$ represents the extraneous noises such as dark current, intensity noise, etc. $n_{thermal}(t)$ and $n_x(t)$ are both arbitrary zero-mean random process, which may be non-white and non-Gaussian.

As, when $P_{LO} >> P_S$, we can see from equation (4.13) that

$$S_n(\omega) \approx \frac{1}{2} qRP_{LO} \tag{4.16}$$

From equation (4.13) if we eliminate DC part by a high pass filter, we can obtain

$$I(t) = R\sqrt{P_S P_{LO}} \cos(\omega_C t + \theta) + n_{shot}(t) + n_{thermal}(t) + n_x(t) \tag{4.17}$$

From equation (4.16) and (4.17) we can see that both the power of desired signal and the main noise are proportional to P_{LO}, therefore increasing P_{LO} will increase bother the signal and the noise. However other noises that we have neglected from equation (4.16) are irrelevant to P_{LO}, thus a higher LO power can reduce the effects of the extraneous noises, and equation (4.17) can be reduced to

$$I(t) \approx R\sqrt{P_S P_{LO}} \cos(\omega_C t + \theta) + n_{shot}(t) \qquad (4.18))$$

This is a so-called *shot-noise-limited* case.

4.4.2 BALANCED COHERENT RECEIVER

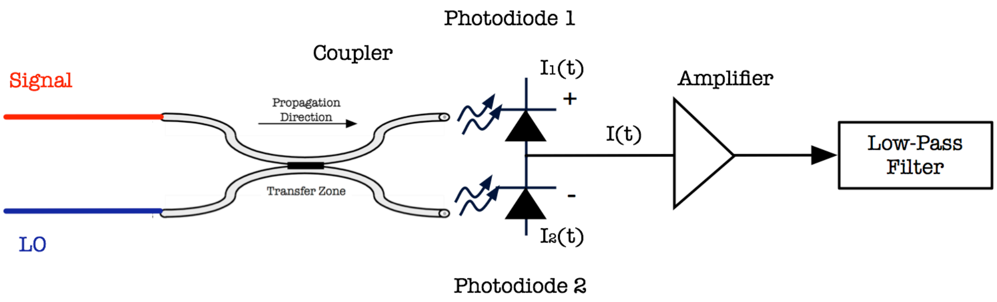


Figure 4.4 Balanced coherent receiver

Figure 4.4 shows a typical structure of single branch coherent receiver that exploits both two outputs of the coupler. Assuming that $P_{LO} >> P_S$, we can have

$$\begin{cases} I_1(t) \approx \frac{1}{2} R\left(P_S + P_{LO} + 2\sqrt{P_S P_{LO}} \cos(\omega_C t + \theta)\right) + n_{shot1}(t) \\ I_2(t) \approx \frac{1}{2} R\left(P_S + P_{LO} - 2\sqrt{P_S P_{LO}} \cos(\omega_C t + \theta)\right) + n_{shot2}(t) \end{cases} \tag{4.19}$$

where $I_1(t)$ and $I_2(t)$ are photocurrents generated by Photodiode 1 and Photodiode 2 and $I(t)$ is the difference between $I_1(t)$ and $I_2(t)$

$$I(t) = I_1(t) - I_2(t) = 2R\sqrt{P_S P_{LO}}\cos(\omega_C t + \theta) + n(t) \tag{4.20}$$

where $n(t) \approx n_{shot1}(t) - n_{shot2}(t)$ is also approximately a zero-mean white Gaussian noise. When optimal detectors are used [2,11], the noise PSD is

$$S_n(\omega) \approx qR(P_{LO} + P_S) \approx qRP_{LO} \tag{4.21}$$

As a matter of fact, the PSDs of the two noise processes add up because the signal field and the LO field have unequal and uncorrelated fluctuations; therefore the photocurrents generated by different photodiodes are thus independent. Another reason is that the coupler does not split photons but randomly distributes them into the two outputs. As a result there is a residual noise on power difference, which can be shown to be equal to the shot noise of a beam of power sum [12,13].

However, the subtraction of the two currents provides the heterodyne or the homodyne signal. The DC term is eliminated completely during the subtraction process when the two branches are balanced in such a way that each branch receives equal signal and LO powers. More importantly, the intensity noise associated with the DC term is also eliminated during the subtraction process. The reason is related to the fact that the same LO provides power to each branch. As a result, intensity fluctuations in the two branches are perfectly correlated and cancel out during subtraction of the two photocurrents. It should be noted that intensity fluctuations associated with the AC term, i.e. the product of the signal of the LO, are not canceled even in a balanced receiver. We also note that the thermal noise, even much smaller than shot noise, cannot be eliminated by balanced configuration since it is related to the characteristics of individual photodiode currents. Nevertheless, their impact is less severe on the system performance because of the square-root dependence of the AC term power on the LO power. Moreover, balanced configuration can allow to double the photocurrent outputs and eliminate the common mode noise, such as imperfect modulation, electrical circuit induced noises, etc.

Balanced receivers are commonly used while designing a coherent lightwave system because of the two advantages offered by them. First, the intensity-noise problem is nearly eliminated. Second, all of the signal and local-oscillator power is used effectively, making it easier to operate in the shot-noise limit.

4.4.3 Performance of Balanced Heterodyne and Balanced Homodyne Detection

In a coherent optical communication system, we can use either frequency modulation or angular modulation.

For a heterodyne system, we can rewrite the equation (4.20) as:

$$I(t) = I_1(t) - I_2(t) = 2R\sqrt{P_S P_{LO}}\cos\left[\omega_C(t)t + \theta\right] + n(t) \tag{4.22}$$

where the carrier angular frequency $\omega_C(t)$ is the intermediate frequency (IF) as frequency modulation, and θ is a constant value. From the equation (4.21), (4.22), with the receiver band width is Δf , the electrical signal-to-noise rate (ESNR) can be given by:

$$ESNR_{Hetero} = \frac{\left\langle I^2(t)\right\rangle}{S_n(\omega) + S_{thermal}(\omega)} \approx \frac{2R^2 P_S P_{LO}}{qRP_{LO}\Delta f} \cdot \frac{1}{2} = \frac{RP_S}{q\Delta f} = \frac{\eta P_S}{hv\Delta f} \tag{4.23}$$

For a homodyne system in which we apply angular modulation and $\omega_C = 0$, we can rewrite the equation (4.20)

$$I(t) = 2R\sqrt{P_S P_{LO}}\cos\left[\theta(t)\right] + n(t) \tag{4.24}$$

where $\theta(t)$ is the phase-shift-keying signal. For a binary phase-shift keying (BPSK) signal, we can deduce from the equations (4.21), (4.24),

$$ESNR_{Homo} = \frac{\left\langle I^2(t) \right\rangle}{S_n(\omega) + S_{thermal}(\omega)} \approx \frac{4R^2 P_S P_{LO}}{2qRP_{LO}\Delta f} = \frac{2RP_S}{q\Delta f} = \frac{2\eta P_S}{hv\Delta f} \tag{4.25}$$

It is more useful to present the ESNR in terms of average photon number per bit N_S. At the bit rate B, the signal power P_S is related to N_S as $P_S = N_S h\upsilon B$, while typically $\Delta f = B/2$. Therefore the equations (4.23), (4.25) can be rewritten as:

$$ESNR_{Hetero} = 2\eta N_S \tag{4.26}$$

$$ESNR_{Homo} = 4\eta N_S \tag{4.27}$$

Now lets consider the Q factor: for a symmetric modulation format, we consider the signal level and noise level of the two symbols 0, 1 as I_0, I_1, σ_0, σ_1. Then we have

$$Q = \frac{I_1 - I_0}{\sigma_1 + \sigma_0} \approx \frac{2I_1}{2\sigma_1} = \left(ESNR\right)^{1/2} \tag{4.28}$$

when the condition $I_0 = -I_1$, $\sigma_0 = \sigma_1$ is used.

Consequently we can obtain the BER performance of both two receivers [14] by using the equation:

$$BER = \frac{1}{2} erfc\left(\frac{Q}{\sqrt{2}}\right) \tag{4.29}$$

For a heterodyne receiver:

$$BER = \frac{1}{2} erfc\left(\sqrt{N_S}\right) \tag{4.30}$$

and for a homodyne receiver:

$$BER = \frac{1}{2} erfc\left(\sqrt{2N_S}\right) \tag{4.31}$$

As a result of the complexity in receiver configurations, the ESNR of homodyne receiver has 3 dB gain compared to heterodyne configuration, leading to a better BER performance, which allows homodyne to reach the quantum limit and more adaptable to weak signal applications, such a phase-modulated QKD system.

4.5 TECHNICAL NOISE AND IMPAIRMENT IN HOMODYNE DETECTION

4.5.1 Classic Phase Fluctuation

In homodyne detection, the local oscillator usually acts as the phase reference for in-phase and in-quadrature definitions. With a phase mismatch $\Delta\theta$ of the local oscillator, the balanced output can be given by [15]:

$$I(t) = 2R\sqrt{P_S P_{LO}}\cos\left[\theta(t) + \Delta\theta\right] + n(t) \tag{4.32}$$

The phase noise is multiplied by the LO field which acts as a lever for classical phase noise effect. Since the obtained output is proportional to the received signal, the noise is no longer simple additive to the quadrature amplitude.

Classical fluctuation appears therefore as a limitation for the signal level, which is an important limitation for strong signal level applications, for instance for QKD using continuous variables.

4.5.2 Phase Diffusion and Line-width

Shawlow and Townes [16], and Lax [17,18] have first pointed out the role of fluctuations in the phase of the optical field on the laser line-width. When concerned by semi-conductor laser (SLC), Henry [19] starts with a corpuscular point of view, in which the instantaneous changes of the phase of the optical field is caused by discrete spontaneous emission events, which discontinuously alter the phase and intensity of the lasing field. Henry's [19] approach points out the importance for SCL of the phase amplitude coupling resulting from deviation of the imaginary part of the refractive index from its steady-state value caused by the change of its real part associated to the gain change and includes an additional phase shift of the laser field. This effect has been previously pointed out by Lax, but was of negligible effect for the laser considered. As intensity fluctuations are smoothed out by gain saturation, the averaged optical phase diffuses in a Brownian motion due to the lack of a restoring force, under the direct and the phase amplitude coupling induced phase changes.

Furthermore, as a critical parameter in coherent detection, the field line-width is not only a property of the quantum noise, but is also the result of the phase diffusion. The electromagnetic wave packets are the classical counter part of the electromagnetic field quantum states. The coherence time is the inverse of the laser line-width that is determined by the laser source and corresponding population inversion, built-in losses, cavity Q factor and phase coupling factor. The laser line-width has also been discussed by Nilsson [20] in terms of quantum noise filtering by the lasing cavity. A continuous-wave (CW) laser, far above threshold, generates a sequence of consecutive nearly coherent states with individual finite time occupancy corresponding to the coherence time. Through the coherent states succession, the phase goes though a random walk, i.e. a Brownian motion, except when a restoring force for the phase is applied by using for instance injection-locking technique [21]. Indeed, phase can never be controlled within the photon number-phase Heisenberg uncertainty, as will be discussed in the next chapter.

Phase diffusion is a natural limitation for interferometric arrangements, in the case of unbalanced recombination of the path acting as LO and the path acting as signal. As first shown by Armstrong [22] and discussed in detail by Gallion and Debarge [23] the homodyne photocurrent spectrum consists, in this case, of two terms, whose behavior relates closely to the normalized time delay, and phase mismatch values. A frequency Dirac function, corresponding to the DC component which stands for the incoherent addition of the two optical powers, and to the amount of remaining phase correlation between the two mixed beams. When the time-delay is large, as compared to the coherence time, we have completely uncorrelated mixed fields and the dependence on the phase matching vanishes out. When the time-delay is small as compared to the coherence time, it becomes very sensitive on phase mismatch values and it no longer depends on the spectral spread, turning into a pure Dirac function, whatever the spectral width is. The second term takes the form of an approximately Lorentzian line shape. It vanishes out for a close to zero delay value. For large delay values, this term is then no longer dependent on the phase matching and stands for the optical mixing of two independent fields and it becomes rigorously Lorentzian with a full width at half maximum (FWHM) which is twice the original laser line width, because the detector acts as an optical product detector, whose output is the autocorrelation product of the laser field spectrum.

4.5.3 Unbalanced Homodyne Detection and Imperfect Quantum Efficiency

Kennedy's [24] binary coherent-state signals receiver uses a homodyne-like configuration with a weak LO whose amplitude is matched to the signal one to produce an unconditional cancellation of one of its antipodal values. Dolinar [25] extended Kennedy's results by allowing the LO to depend on the observed output of the photodetector. This structure is an explicit realization of the optimum quantum receiver for phase-shift-keying (PSK) signals. For such a "one output port" single detector homodyne arrangement also has been discussed by Yuen et al. [26]: the amplitude splitting coefficients $\sqrt{\varepsilon}$ and $\sqrt{1-\varepsilon}$ are selected to be respectively equal to 1 and 0 and a theoretically infinite power of a local oscillator is required to surmount thermal noise.

For the 2 port arrangement, proposed by Yuen [27] and also discussed by Shapiro [28], the exact intensity cancellation condition of a LO noise is $\varepsilon = ½$. Any attenuation in a balanced homodyne arrangement can be expressed, without loss of generality, by an intensity transmission coefficient $T < 1$. Attenuation destroys the balance in the two arms and produces an amplitude attenuation of the measured quadrature by a factor $\sqrt{T}$, and meanwhile introducing an additional constant level noise, i.e. Gaussian attenuation noise with a spectral density $\sqrt{1-T}\,h\nu/2$.

A balanced mixer achieves the quantum-limited operation only when the two photodetectors' quantum efficiencies are identical and equal to unity. For non-ideal photodetectors with quantum efficiencies η_1 and η_2 the corresponding signal penalties are introduced. However Machida [29] points out that an exact local oscillator intensity noise cancellation condition can be preserved, by using $\eta_1(1-\varepsilon) = \eta_2\varepsilon$.

4.6 QUANTUM THEORY OF HOMODYNE DETECTION

Coherent detection is a well-known method using the non-linear mixing, via a square-law detector, of the signal field and a reference field so-called the local field (LO). When the frequencies of the two mixed fields are different, it is usually referred as heterodyne detection; and as homodyne detection when the two frequencies are identical. Heterodyne detection allows a passband recovery of the signal information centered at the frequency difference between the two mixed fields, so-called the intermediate frequency (IF), which leads to an easy-to-implement post-detection information processing free of low-frequency noise and fluctuations. In optical interferometry, homodyne corresponds to the generation of the LO field from the beam splitting of the same source where signal field is generated. Such an arrangement is insensitive to frequency fluctuations from the common field source, except those occurring on a time scale larger than the usually short delay due to unequal interferometer paths, resulting in decoherence. In coherent detection the signal field is usually weak, as compared to the local one, and a strong and noise free mixing gain can thus be obtained.

Homodyne detection, as a process in which the signal benefits from a noise free mixing gain with LO, can be easily processed, i.e. amplified, filtered, and synchronized. Furthermore, homodyne receiver structures are flexible to be designed for phase diversity, polarization diversity, and polarization division multiplexing, either with separated LO or in self-homodyne configurations. Recently fast digital signal processing techniques for performing these operations have been reported experimentally, allowing to overcome several impairments in the optical channel, such as phase synchronization in a feed-forward configuration and fiber linear and non linear phase dispersion compensation.

For the quantum states discrimination in a binary channel, homodyne detection consists of a quantum mechanical Gaussian operation: mapping input quantum states into Gaussian states $\rho = \xi_1 |\alpha\rangle\langle\alpha| + \xi_2 |-\alpha\rangle\langle-\alpha|$. Takeoka [30] and Nha and Carmichael [31] have proved that homodyne measurement is the best strategy to discriminate among binary coherent states with Gaussian operations, and that any classical operation. In the case of more complex constellations with coherent states, i.e. M-ary modulations, further analysis is required. Indeed distinguishing among an ensemble of states can be conceptualized as a problem of realizing minimum overlap among states.

The balanced homodyne detection (BHD) scheme detects the field superposition at the two output ports of the 50/50 coupler and the subsequent electronic subtraction cancels out the photon number sum at the input ports from the detected fields. Semi-classical analysis of the BHD have been made by Abbas, Chan and Yee [32], demonstrating the property of canceling the local oscillator excess noise, but still interpreting the quantum limit as the result of the LO shot noise. Yuen and Chan [27], Shumaker [33] and also Collett, Loudon and Gardiner [34] for fields of general quantum state, introduced a quantum mechanical treatment, interpreting the BHD as canceling both the LO excess and quantum noises, demonstrating that the quantum limit is the signal quantum fluctuation. Extended analysis on imperfect time/frequency overlap between signal and local oscillators has been conducted by Grosshans and Grangier [35].

Under the conditions of ideal coupler and detectors, with LO in a strong coherent state having a relative phase shift θ to the received signal eigenstate $|x\rangle$, the quantum observable is the field quadrature [15]:

$$\hat{x}_\theta = \frac{\exp(j\theta)\hat{a}^+ + \exp(-j\theta)\hat{a}}{\sqrt{2}} \tag{4.33}$$

In fact, the ideal BHD is a quantum measurement of the field quadrature defined as the intrinsic homodyne quantum observable $\left| x_\theta \right\rangle$, consisting of the signal quadrature distribution rescaled by the amplitude of the LO. For imperfect BHD, lossy couplers and non-unit efficiency detectors add vacuum noise that would result in Gaussian spread of the quadrature measurement.

Now let us consider the homodyne detection of a signal with a local oscillator fields respectively described by the quantum photon annihilation operators $\hat{s}$ and $\hat{l}$. The two fields are first assumed combined by using a lossless and a perfectly balanced coupler as depicted on Figure 4.5.

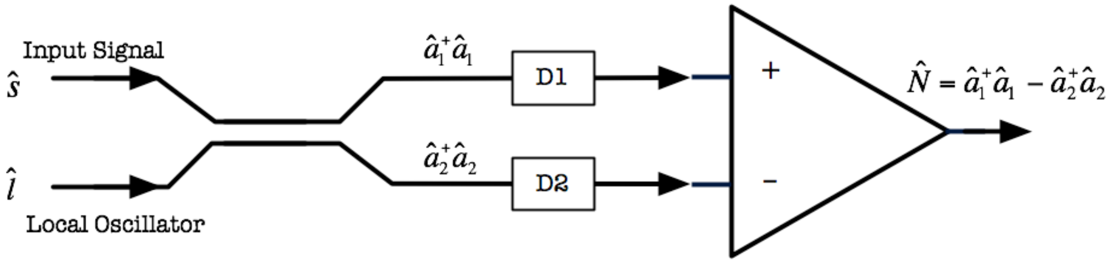


Figure 4.5 Homodyne detection arrangement

According to the coupler transfer matrix the resulting field on detector D_1 and D_2 are:

$$\hat{a}_1 = \frac{1}{\sqrt{2}}\left(\hat{s} - j\hat{l}\right),\ \hat{a}_2 = \frac{1}{\sqrt{2}}\left(-j\hat{s} + \hat{l}\right) \tag{4.34}$$

and the associated the photon number operators are respectively

$$\hat{a}_1^+\hat{a}_1 = \frac{1}{2}\left(\hat{s}^+\hat{s} + \hat{l}^+\hat{l} - j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right)\right) \text{ and } \hat{a}_2^+\hat{a}_2 = \frac{1}{2}\left(\hat{s}^+\hat{s} + \hat{l}^+\hat{l} + j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right)\right) \tag{4.35}$$

The coherent subtraction of the 2 photocurrents outputs allows us to take benefit of the signal and LO interaction spread on the 2 detectors by the combiner. Assuming perfect quantum efficiency for the two detectors D1 and D2, the photoelectron number operator is equal to the photon number operator for each detector; hence the electron number operator for the subtraction output current is given by

$$\hat{N} = \hat{a}_1^+\hat{a}_1 - \hat{a}_2^+\hat{a}_2 = -j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right) \tag{4.36}$$

Using signal and LO field operator expansions in terms of in-phase and quadrature Hermitian components, we have:

$$\hat{s} = \hat{s}_I + j\hat{s}_Q \text{ and } \hat{l} = \hat{l}_I + j\hat{l}_Q \tag{4.37}$$

therefore,

$$\hat{N} = 2\left(\hat{s}_I\hat{l}_Q - \hat{s}_Q\hat{l}_I\right) \tag{4.38}$$

Note that in this description, $\hat{s}$ and $\hat{l}$ refer to the fields at the input of the optical combiner and that, despite their different index, $\hat{s}_I$ and $\hat{l}_Q$ (or $\hat{s}_Q$ and $\hat{l}_I$) refer to the same quadrature at the detector input, according to the phase shift property of the optical combiner. We can thus simplify the notation, by referring the phase of the local oscillator field on the detector 1, i.e. in the above equations we replace $-j\,\hat{l}$ by $\hat{l}$ and then we obtain [26]:

$$\hat{N} = \hat{s}^+\hat{l} - \hat{l}^+\hat{s} = 2\left(\hat{s}_I\hat{l}_I + \hat{s}_Q\hat{l}_Q\right) \tag{4.39}$$

Note that $\hat{N}$ is twice the projection of the signal operator on the local field operator. Here we will restrict our analysis to the case where both the LO and signal fields are single coherent states. Assuming that the signal and the LO fields are coherent states, we can thus separate the classical and quantum contributions for the 2 quadratures of the signal and the local oscillator field:

$$\begin{gathered}\hat{s}_I = S_I + \Delta\hat{s}_I \text{ with } S_I = \left\langle \hat{s}_I \right\rangle \text{ and } \hat{s}_Q = S_Q + \Delta\hat{s}_Q \text{ with } S_Q = \left\langle \hat{s}_Q \right\rangle \\ \hat{l}_I = L_I + \Delta\hat{l}_I \text{ with } L_I = \left\langle \hat{l}_I \right\rangle \text{ and } \hat{l}_Q = L_Q + \Delta\hat{l}_Q \text{ with } L_Q = \left\langle \hat{l}_Q \right\rangle\end{gathered} \tag{4.40}$$

To detect S_I (or S_Q) we have to set L_Q (or L_I) to zero. Assuming that S_I is to be detected, and the LO acts as the phase reference for the signal, we can obtain

$$\hat{N} = 2\left(\left(L_I + \Delta\hat{l}_I\right)\left(S_I + \Delta\hat{s}_I\right) + \Delta\hat{l}_Q\left(S_Q + \Delta\hat{s}_Q\right)\right) \tag{4.41}$$

For strong LO level $N_L = L_I^2 >> N_S = S_I^2 + S_Q^2$, the dominating term is

$$\hat{N} = 2\hat{s}_I\hat{l}_I = 2\left(S_I + \Delta\hat{s}_I\right)L_I \tag{4.42}$$

Here we have neglected quantum fluctuations of the LO since they are added to its deterministic part and have no cross product with it.

The output signal of a balanced homodyne detection arrangement is proportional to the quadrature S_I and its additional quantum noise $\Delta\hat{s}_I$. Its input signal is amplified by the deterministic part of the LO in-phase quadrature on the detectors that provides a noise free mixing gain. Actually in homodyne detection only one quadrature is measured and no noise addition to the zero-point fluctuation of the signal field is introduced, therefore the input signal quantum noise is the only noise limitation. The LO noise has a negligible influence and the output noise is only governed by the vacuum fluctuation entering into the signal port. The limitation of the output noise of homodyne detector, has been experimentally confirmed at quantum level by Machida and Yamamoto [29]. They also point out the difficulty to verify if the quantum noise of a LO wave can be cancelled as well as its excessive noise, when the signal and the LO waves possessed the same amount of quantum noise. A squeezed state input signal is required in order to clarify this point and to completely refute the semi-classical description based on the local oscillator shot noise.

Assuming a perfectly phase matched LO, free of relative phase fluctuations with respect to the signal, the overall photon number operator is

$$\hat{N} = \left\langle \hat{N} \right\rangle + \Delta\hat{N} \text{ with } \left\langle \hat{N} \right\rangle = 2L_I S_I \text{ and } \Delta\hat{N} = 2L_I\Delta\hat{s}_I \tag{4.43}$$

The average photon number is equal to the average electron number assuming unit quantum efficiency. The square electron number is

$$\hat{N}^2 = 4L_I^{\ 2}\left\langle S_I^{\ 2} + \left(\Delta\hat{s}_I\right)^2\right\rangle \tag{4.44}$$

Assuming that the signal and LO are coherent states, denoted by $\left|\alpha_S\right\rangle$ and $\left|\alpha_L\right\rangle$ respectively, and a constant envelope modulation is used for the signal. The average signal and local photon number N_S and N_L are defined as

$$N_S = \left\langle \hat{s}^+\hat{s}\right\rangle = \left|\alpha_{\mathrm{S}}\right|^2 \ \text{ and } N_L = \left\langle \hat{l}^+\hat{l}\right\rangle = \left|\alpha_{\mathrm{L}}\right|^2 \tag{4.45}$$

We can thus obtain

$$\left\langle \hat{N}^2\right\rangle = \left\langle \hat{N}\right\rangle^2 + \left\langle\left(\hat{N}\right)^2\right\rangle = 4L_I^{\ 2}\left(S_I^{\ 2} + \frac{1}{4}\right) = 4N_LN_S + N_L \tag{4.46}$$

The first term of the left hand side of the equation (4.42) is the averaged square of the signal photon number, while the second term is the averaged square of the photon number fluctuations

$$\left\langle \hat{N}\right\rangle^2 = 4N_LN_S \ \text{ and } \ \left\langle\left(\Delta\hat{N}_L\right)^2\right\rangle = N_L \tag{4.47}$$

The second part of Equation (4.43) is the well-known Poisson fluctuation relationship, in agreement with the classical theory of homodyne detection, which will be discussed below and for which the fundamental noise limitation is interpreted as the LO shot noise. The signal to noise ratio (SNR) is given by

$$SNR = \frac{4N_LN_S}{N_L} = 4N_S \tag{4.48}$$

In digital communication systems it is common to express the SNR in term of the energy per bit E_B divided by the single sided spectral density N_0, i.e. the ratio E_B/N_0. It is a normalized signal-to-noise ratio measure, also known as the SNR per bit. Denoting the bit duration T, i.e. the observation time, and we assume that a matched electrical filter with equivalent bandwidth $B_E = 1/2T$ is used. Since the homodyne beating signal is in the base-band, the optical bandwidth B_O is identical to the electrical one, hence the signal to noise ratio can also be expressed as a function of the averaged optical signal power P_S, in the form of [36].

$$SNR = \frac{P_S}{\frac{h\nu}{2} B_O} = 2\frac{E_B}{N_0} \tag{4.49}$$

The single sided spectral density of noise N_0 is equal to the zero point fluctuation of the optical field $S_{N0} = h\nu/2$. The signal to noise ratio per bit is especially useful when comparing the BER performance of different digital modulation schemes without taking the bandwidth consideration into account. It is equal to the SNR divided by the link spectral efficiency in bit/s/Hz, which is $R/B_0 = 2$ in our case, where the bit rate $R = 1/T$ is independent of error correction overhead or modulation symbols.

REFERENCES

1. K. C. Kao, and G. A. Hockham, “Dielectric-fibre surface waveguides for optical frequencies”, *IEE proceedings: Part Journal of Optoelectronics* **113**, 1151--1158 (1966).
2. J. R. Barry, and E. A. Lee, “Performance of coherent optical receivers”, *Proceedings of the IEEE* **78**, 1369--1394 (1990).
3. E. Basch, T. Brown, “Introduction to coherent optical fiber transmission”, *IEEE Communications Magazine* **23**, 23--30 (1985).
4. J. Salz, “Modulation and detection for coherent lightwave communications”, *IEEE Communications Magazine* **24**, 38--49 (1986).
5. R. Loudon, *The Quantum Theory of Light*, Chapter 6.10, (Oxford Science Publications 2000).

6. K.-P. Ho, *Phase-Modulated Optical Communication Systems*, (Springer 1st edition 2005).

7. T. Okoshi, K. Kikuchi, *Coherent Optical Fiber Communications (Advances in Opto-Electronics)*, (Springer 1988).

8. S. Betti, G. D. Marchis, E. Iannone, *Coherent Optical Communications Systems*, (Wiley-Interscience 1995).

9. S. Ryu, *Coherent Lightwave Communication Systems*, (Artech House Publishers 1995).

10. A. H. Gnauck, and P. J. Winzer, "Optical phase-shift-keyed transmission", *Journal of Lightwave Technology* **23**, 115--130 (2005)

11. I. B. David, and J. Salz, "On dual optical-detection – homodyne and transmitted-reference heterodyne reception", *IEEE Transaction of Communications* **36**, 1309--1315 (1988).

12. J. J. Snyder, E. Giacobino, C. Fabre, A. Heidmann, and M. Ducloy, "Sub-shot-noise measurements using the beat note between quantum-correlated photon beams", *Journal of Optical Society of America B* **7**, 2132--2136 (1990).

13. F. Jeremie, J. L. Vey, and P. Gallion, "Optical corpuscular theory of semiconductor laser intensity noise and intensity squeezed-light generation", *Journal of the Optical Society of America B* **14**, 250-257 (1997).

14. P. Agrawal, *Fiber-Optic Communication Systems*, chapter 10.4.2, (3rd edition Wiley-Interscience 2002).

15. P. Gallion, F.J. Mendieta, and S. Jiang, “Signal and quantum noise in optical communcation and in cryptography”. Elsevier 2008, to be published in *Progress in Optics* **52** (2008).

16. A. L. Shawlow, and C. H. Townes, “Infrared and optical masers”, *Physical Review* **112**, 1940--1949 (1958).

17. M. Lax, “Classical noise V. noise in self-sustained oscillators”, *Physical Review* **160**, 290--307 (1967).

18. M. Lax, “Quantum noise X. density-matrix treatment of field and population-difference fluctuations”, *Physical Review* **157**, 213--231 (1967).

19. C. H. Henry, “Theory of the line width of semiconductor lasers”, *IEEE Journal of Quantum Electronics* **18**, 259--264 (1982).

20. B. O. Nilsson, “Noise mechanisms in laser diode”, *IEEE Transactions on Electron Devices* **41**, 2139--2150 (1994).

21. P. Gallion, H. Nakajima, G. Debarge and C. Chabran, “Contribution of spontaneous emission to the linewidth of an injection locked semiconductor laser”, *Electronics Letters* **21**, 626--627 (1985).

22. J. A. Armstrong, “Theory of interferometric analysis of laser phase noise”, *Journal of Optical Society of America* **56**, 1024--1031 (1966).

23. P. Gallion, and G. Debarge, “Quantum phase noise and field correlation in single frequency semiconductor laser systems”, *IEEE Journal of Quantum Electronics* **20**, 343--349 (1984).

24. R. S. Kennedy, “A near-optimum receiver for the binary coherent state quantum channel”, *Quarterly Progress Report* **108**, Research Laboratory of Electronics MIT, 219--225 (1973).

25. S. Dolinar, “An optimum receiver for the binary coherent state quantum channel”, *Quarterly Progress report* **111**, Research Laboratory of Electronics MIT, 115--120, (1973).

26. H. P. Yuen, and J. H. Shapiro, “Optical communication with two-photon coherent states-Part III: Quantum measurement realizable with photo emissive detectors”, *IEEE Transaction of Information Theory* **26**, 78--92 (1980).

27. H. P. Yuen, and V. W. S. Chan, “Noise in homodyne and heterodyne detection”, *Optics Letters* **8**, 177--179 (1983).

28. J. H. Shapiro, “On the near-optimum binary coherent-state receiver”, *IEEE Transactions on Information Theory* **26**, 490--491 (1980).

29. S. Machida, and Y. Yamamoto, “Quantum-limited operation of balanced mixer homodyne and heterodyne receivers”, *IEEE Journal of Quantun Electronics* **22**, 617--624 (1986).

30. M. Takeoka, and M. Sasaki, “Discrimination of the binary coherent signal: Gaussian limit and simple non-Gaussian near-optimal receivers”, *Physical Review A* **78**, 022320 (2007).

31. H. Nha, and H. J. Carmichael, “Distinguishing two single-mode Gaussian states by homodyne detection: An information-theoretic approach”, *Physical Review A* **71**, 032336 (2005).

32. G. L. Abbas, V. W. S. Chan, and T. K. Yee, “Local-oscillator excess-noise suppression for homodyne and heterodyne detection”, *Optics Letters* **8**, Issue 8, 419-421 (1983).

33. B. L. Schumaker, “Noise in homodyne detection”, *Optical Letters* **9**, 189-191 (1982).

34. M. J. Collett, R. Loudon, and C.W.Gardiner, *Quantum theory of optical homodyne and heterodyne detection, Journal of Modern Optics* **34**, Nos. 6-7, 881-902 (1987).

35. F. Grosshans, and P. Grangier, “Effective quantum efficiency in the pulsed homodyne detection of a n-photon state”, *The European Physical Journal D* **14**, 119-125 (2001).

36. J. G. Proakis, *Digital Communications*, third edition. McGraw-Hill Inc., New York (1995).

CHAPTER 5 PHASE ENCODING ON WEAK COHERENT STATES AND QUANTUM DETECTION

5.1 CLASSICAL ELECTROMAGNETIC WAVE DESCRIPTION

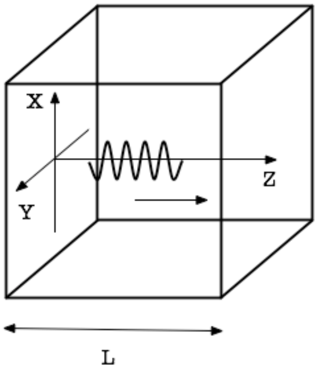


Figure 5.1 Electric field of an electromagnetic wave polarized in the x-direction enclosed in a cavity of dimension L

A classical monochromatic wave that is plane-polarized in the x-axis and propagates in the direction z-axis within a cavity of mode area A and length L, we can write down the electric field in the following form:

$$e_x(z,t) = e_0 \sin kz \sin(\omega t + \phi) \qquad (5.1)$$

where e_0 is the amplitude, $k = 2\pi / \lambda$ is the wave vector, and ω is the angular frequency, and ϕ is a phase factor. The electric field energy for the field given in the equation (5.1) is equal to:

$$\begin{aligned} E_{electric} &= \frac{1}{2}\varepsilon_0 A \int_0^L e_0^2 \sin^2 kz \sin^2(\omega t + \phi) dz \\ &= \frac{1}{4}\varepsilon_0 A L e_0^2 \sin^2(\omega t + \phi) \\ &= \frac{1}{4}\varepsilon_0 V e_0^2 \sin^2(\omega t + \phi) \end{aligned} \tag{5.2}$$

where ε_0 is the vacuum permittivity and $V = AL$. And we can extend the equation (5.1) as:

$$\begin{aligned} e_x(z,t) &= e_0 \sin kz(\cos\phi \sin\omega t + \sin\phi \cos\omega t) \\ &= e_1 \sin\omega t + e_2 \cos\omega t \end{aligned} \tag{5.3}$$

The amplitudes of the two field quadratures corresponding to the two oscillating fields are $e_1 = e_0 \sin kz \cos\phi$, $e_2 = e_0 \sin kz \sin\phi$, respectively.

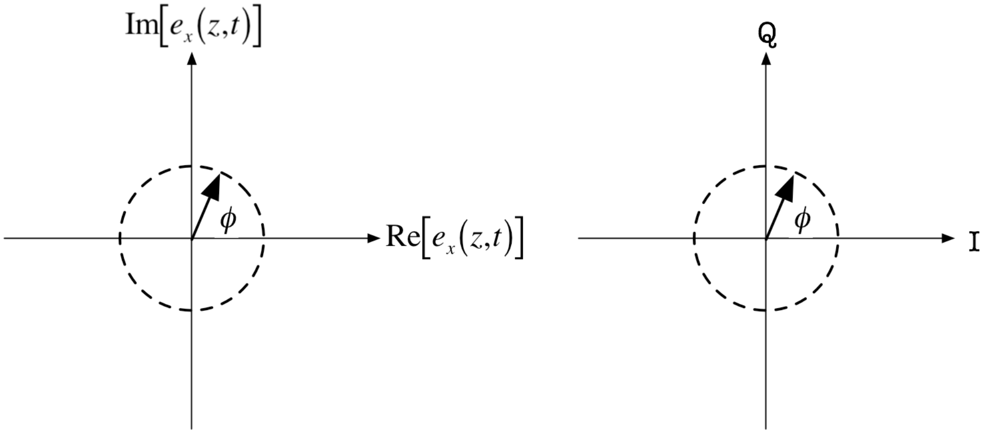


Figure 5.2 Phasor diagram for a classical wave of amplitude e_x

In quantum optics, it is more convenient to work in unit in which the field is dimensionless. As the energy unit of photon is hv where $v = \dfrac{\omega}{2\pi}$ is the wave frequency, the normalized in-phase (I) amplitude and quadrature (Q) amplitudes are:

$$\begin{cases} X_I(t) = \left(\dfrac{\varepsilon_0 V}{4hv}\right)^{1/2} e_0 \sin(\omega t + \phi) \\ X_Q(t) = \left(\dfrac{\varepsilon_0 V}{4hv}\right)^{1/2} e_0 \cos(\omega t + \phi) \end{cases} \tag{5.4}$$

As the Heisenberg uncertainty principle [1,2] for the quantum uncertainty of the position and momentum, the field quadrature amplitudes are subject to quantum uncertainty in exact the same way for the I-Q amplitudes [3]:

$$\Delta X_I \Delta X_Q \geq \frac{1}{4} \tag{5.5}$$

5.2 VACUUM STATE

The well known quantized harmonic oscillator theory give corresponding energy level:

$$E_n = \left(n + \frac{1}{2}\right)hv \tag{5.6}$$

The energy is quantized and can only take discrete values, such as $\frac{1}{2}hv$, $\frac{3}{2}hv$, $\frac{5}{2}hv$ and so forth since *n* is an integer [4,5].

Vacuum *state* is the quantum state with the lowest possible energy. The term “ground state energy” or “zero-point field” is sometimes used as a synonym for the vacuum state of an individual quantized field. The vacuum energy or the vacuum expectation value of the energy is the quantization of a simple harmonic oscillator states that the lowest possible energy or zero-point energy that such an oscillator may have is $E_{vacuum} = \frac{1}{2}hv$. In the vacuum state, according to quantum mechanics, an oscillator performs null oscillations and its average kinetic energy is positive.

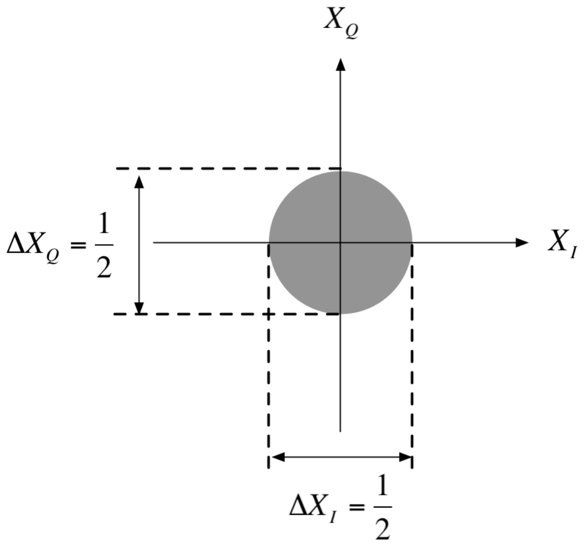


Figure 5.3 Phase diagram for the vacuum state

The zero-point energy originates from a randomly fluctuating electric field, and the classical field amplitude e_0 is zero for the vacuum state. Therefore the vacuum state can be represented on a phasor diagram as uncertainty circle centered at the origin as shown in Figure 5.3. The shaded region indicates the random fluctuation of the field. The uncertainties in the two quadratures are identical, induced by zero-point half photon energy fluctuation; both are equal to the minimum value allowed by the equation (5.5):

$$\Delta X_I = \Delta X_Q = \frac{1}{2} \tag{5.7}$$

5.3 COHERENT STATE

In quantum mechanics a *coherent state* $|\alpha\rangle$ is a specific kind of quantum state of the quantum harmonic oscillator that is an equivalent of a classical monochromatic electromagnetic wave [5-7]. $\alpha = |\alpha|e^{j\phi}$ is a *dimensionless* complex number that can be understood by considering a linearly polarized mode of angular frequency ω enclosed within a cavity of volume V. α can be defined as:

$$\alpha = \alpha_I + i\alpha_Q \tag{5.8}$$

with the vector length:

$$|\alpha| = \sqrt{\alpha_I{}^2 + \alpha_Q{}^2} \tag{5.9}$$

and

$$\begin{cases} \alpha_I = |\alpha|\cos\phi \\ \alpha_Q = |\alpha|\sin\phi \end{cases} \tag{5.10}$$

According to these definitions, we can represent the coherent state $|\alpha\rangle$ as shown in Figure 5.4. For classical state of light, there is no intrinsic preference to either of the two quadratures, and their uncertainty must be identical $\Delta X_I = \Delta X_Q = \dfrac{1}{2}$.

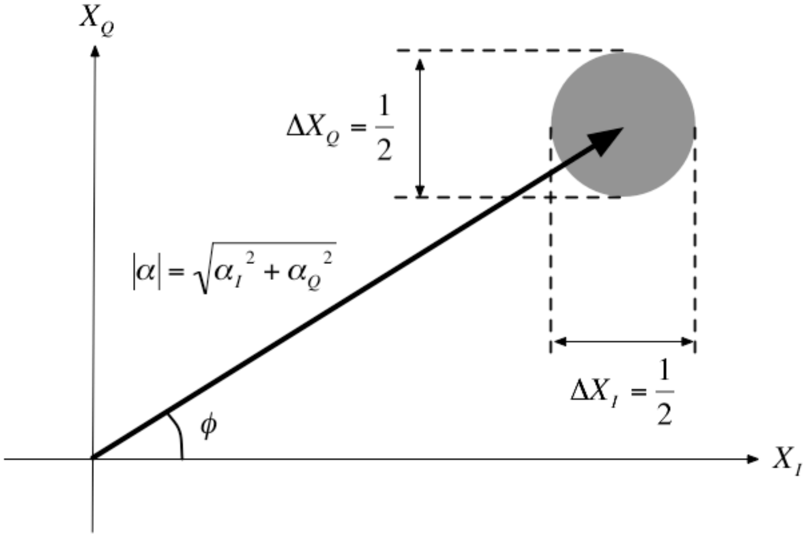

X_Q
$\Delta X_Q = \frac{1}{2}$
$|\alpha| = \sqrt{\alpha_I{}^2 + \alpha_Q{}^2}$
$\Delta X_I = \frac{1}{2}$
ϕ
X_I

Figure 5.4 Phasor diagram for the coherent state $|\alpha\rangle$

Hence, coherent states can be considered as vacuum states displaced from the origin zero-point to the field vector $|\alpha\rangle$, with the uncertainty circle of vacuum states. If $\overline{n}$ is the average photon number excited in the cavity, and the classical energy definition is

$\overline{E_{energy}} = \bar{n}h\nu$, then the average length value of $|\alpha\rangle$ will be $\overline{|\alpha|} = \sqrt{\bar{n}}$ with equal uncertainty on the two quadratures, limited by zero-point energy fluctuation.

The additive random noise of the coherent state $|\alpha\rangle$ can be written as: $\Delta\alpha(t) = \Delta\alpha_I(t) + i\Delta\alpha_Q(t)$. $\Delta\alpha$ is Gaussian as well as its independent in-phase $\Delta\alpha_I(t)$ and in-quadrature $\Delta\alpha_Q(t)$ components. These two components are uncorrelated base-band noise process with bandwidth $B_o/2$ and have the same single-sided spectral power density S_N as the total noise $\Delta\alpha(t)$ [8]. The probability distributions for the independent in-phase and quadrature noise components are

$$p(\alpha_{I/Q}) = \frac{1}{\sigma\alpha_{I/Q}\sqrt{2\pi}} \exp - \frac{\left(X_{I/Q} - \langle X_{I/Q}\rangle\right)^2}{2\sigma\alpha_{I/Q}^2} \tag{5.11}$$

with $\sigma\alpha_I^2 = \sigma\alpha_Q^2 = S_N \dfrac{B_O}{2}$.

The total average noise power can be obtained as:

$$P_N = \frac{h\nu}{2} B_O \tag{5.12}$$

This additive noise, which accompanies any optical field, is usually referred in quantum electrodynamics, to the zero-point field fluctuations or the vacuum fluctuations. The addition of the zero-point field fluctuations to a classical deterministic field is an intrinsic property making the coherent state of the light a stochastic process whether the light is modulated or not.

We can consider quantum fluctuations as produced by an additive white Gaussian noise (AWGN) noise with the single sided spectral density, in the considered signal polarization mode:

$$S_{N0} = h\nu/2 \tag{5.13}$$

This noise is only observable through its cross term product with another signal and is not directly observable. By using $B_O = 1/T$, the energy $h\nu/2$ can be interpreted as the minimum detectable value of the energy for an observation time *T*. This value is also the minimum value $E_0 = h\nu/2$ of the quantified energy $E_n = (n + 1/2)h\nu$ of a harmonic oscillator, which is always present but not available for exchange. For ν =193 Thz, corresponding to the minimum attenuation of silica fiber and to the center of amplification range of EDFA, corresponding to the so-called communication wavelength of 1550 nm, the zero-point field spectral density S_{N0} is 0.65×10^{-19} W/Hz. Vacuum fluctuations are additive for the field and are already present at any (evenly unused) signal input optical amplifier, an optical coupler etc. They include phase and amplitude (or intensity) noise as well.

5.4 PHASE-NUMBER UNCERTAINTY AND SHOT NOISE

From the equations (5.9) and (5.10) we can see that both the length and angle of the coherent stat are uncertain.

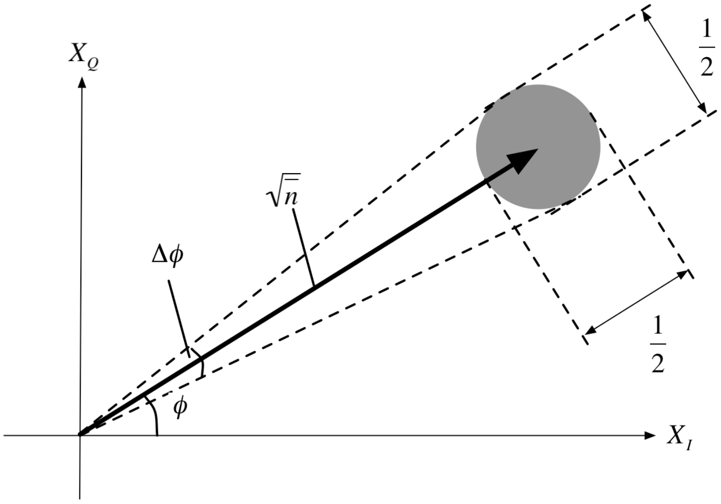


Figure 5.5 The phase-number uncertainty circle of coherent states

We first consider the photon number uncertainty [9-11], as the circle diameter is $\frac{1}{2}$, it is evident that the vector length is uncertain between $(\alpha + 1/4)$ and $(\alpha - 1/4)$. Hence we have:

$$\Delta n = (|\alpha| + 1/4)^2 - (|\alpha| - 1/4)^2 = |\alpha| = \sqrt{n} \tag{5.14}$$

This result also conforms to the Poisson photon statistics as mentioned in Chapter 4. We have mentioned that the shot noise is caused by the Poisson statistics of the laser source. The equation (5.14) points out that the in the optical detection, the observed shot noise is induced by the quantum uncertainty.

As for the phase uncertainty $\Delta\phi$, we can obtain easily from Figure 5.5 that $\sin\left(\frac{\Delta\phi}{2}\right) = \frac{1}{4\sqrt{n}}$, hence we have

$$\Delta\phi = 2\sin^{-1}\left(\frac{1}{4\sqrt{n}}\right) \tag{5.15}$$

As we can see from Figure 5.6 when $\overline{n} = 0$, i.e. for the vacuum states, the phase ϕ can't be measured and has the maximum uncertainty value π; and uncertainty $\Delta\phi$ decreases with higher $\overline{n}$. Also in the Figure 5.7 we can see, when $\overline{n} >> 1$, the phase-number uncertainty is lower bounded by $\frac{1}{2}$.

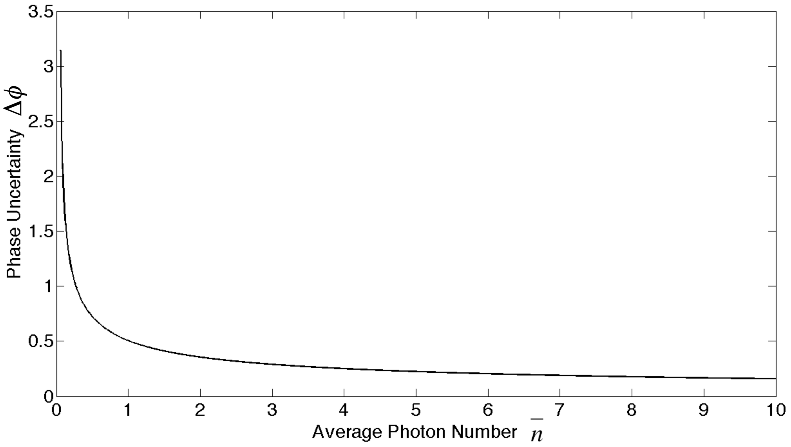


Figure 5.6 The phase uncertainty evaluation with $\bar{n}$

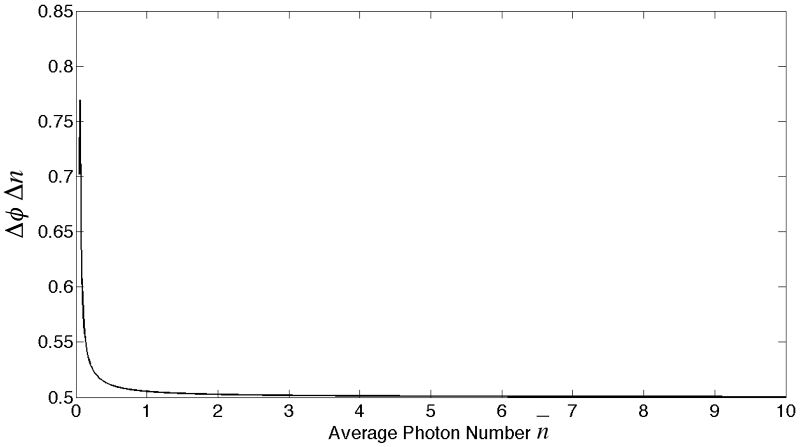


Figure 5.7 The phase-number uncertainty relation

Thus the phase-number uncertainty relationship is:

$$\Delta\phi\Delta n \geq \frac{1}{2} \tag{5.16}$$

This relationship shows that it is impossible to obtain perfect precision on the phase and on the photon number of a lightwave at the same time [11].

Furthermore, when only the quantum noise is considered, this rule permits a practical method for estimating the mean photon number N_S of signals consisting of coherent states in the homodyne detection: with the vacuum state fluctuation ΔX that corresponds to half photon energy, and the measured quadrature amplitude value X that corresponds to $\sqrt{N_S}$, we can have:

$$\frac{X}{\Delta X} = \frac{\sqrt{N_S}}{1/2} \Rightarrow N_S = \left(\frac{X}{2\Delta X}\right)^2 \tag{5.17}$$

5.5 QUANTUM DETECTION

The pioneering works on quantum detection and estimation theory by Helstrom [12], Yuen and Kennedy [13], Hirota and Tsushima [14], and Belavkin [15] for the digital channel, were based on quantum hypothesis testing: in this theory the detection process consists of a generalized quantum measurement which is mathematically described by a probability operator value measurement (POVM) in the following way: given an M-ary received signal, whose states have *a priori* probabilities ξ_m and density operators $\hat{\rho}_m,\ m = 1...,M$ consisting of a unit trace, non-negative Hermitian operators, i.e. $\hat{\rho}_m \geq 0, \forall m$ and $tr\hat{\rho}_m = 1, \forall m$, where *tr* stands for the trace of the operator matrix. The POVM is a detection operator $\hat{\Pi}_l, l = 1,...,M$ that possesses the following properties:

- Positiveness: $\hat{\Pi}_l \geq 0 \forall l$ (5.18)

- Completeness: $\sum_{l=1}^{M} \hat{\Pi}_l = \hat{I}$ (5.19)

where $\hat{I}$ is the identity operator. Such as the conditional probability of inferring that a measurement output signal in the *m* state corresponds to a signal in the *l* state is:

$$\Pr(l/m) = tr(\hat{\Pi}_l \hat{\rho}_m) \tag{5.20}$$

This is the probability of choosing the hypothesis H_m when H_l is true; therefore the probability of error also called the bit error ratio (BER), is obtained in terms of the POVM:

$$BER = 1 - \sum_{m=1}^{M} \xi_m tr\hat{\rho}_m \hat{\Pi}_m \tag{5.21}$$

Helstrom [16] introduced the quantum statistical detection theory for optimal decision among several hypotheses: for the case of binary signals consisting of pure states ψ_0 and ψ_1, there are two density operators labeled $\rho_0 = |\psi_0\rangle\langle\psi_0|$ and $\rho_1 = |\psi_1\rangle\langle\psi_1|$, with prior probabilities ξ_0 and ξ_1, with $\xi_0 + \xi_1 = 1$; the two hypothesis are labeled H_0 and H_1.

In this approach a POVM operator $\left\{\hat{\Pi}, \hat{I} - \hat{\Pi}\right\}$ is applied, obtaining the following probabilities:

$$\Pr(H_1/H_1) = tr(\rho_1\Pi) \qquad \text{(detection probability)} \tag{5.22}$$

$$\Pr(H_1/H_0) = tr(\rho_0\Pi) \qquad \text{(false alarm probability)} \tag{5.23}$$

And the average probability of error is obtained from:

$$BER = \xi_0 \Pr(H_1/H_0) + \xi_1\left[1 - \Pr(H_1/H_1)\right] \tag{5.24}$$

Based on the statistical Neyman Pearson criterion for the maximization of the detection probability, Helstrom [16] finds the minimum attainable error probability so-called the Helstrom bound:

$$BER = \frac{1}{2}\left\{1 - \sqrt{1 - 4\xi_0\xi_1\left|\langle\psi_1|\psi_0\rangle\right|^2}\right\} \tag{5.25}$$

Thus depending on the inner product $\langle\psi_1|\psi_0\rangle$, this probability is obviously lower when the quantum states are more orthogonal to each other.

5.6 BSPK ENCODING AND PERFORMANCE

Glauber's coherent states model can be expressed as a sum of Fock's number states $\left|n\right\rangle$. We can represent in use the form [6]:

$$\left|\alpha\right\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{(n!)^{1/2}}\left|n\right\rangle \tag{5.26}$$

Two coherent quantum state vectors $\left|\alpha_1\right\rangle$ and $\left|\alpha_2\right\rangle$ are non-orthogonal, since the signal overlap is:

$$\begin{aligned}\left\langle\alpha_1|\alpha_2\right\rangle &= \left|e^{-\frac{\left(|\alpha_1|^2+|\alpha_2|^2\right)}{2}}\sum_n\sum_m\frac{\alpha_1^n}{\sqrt{n!}}\frac{\alpha_2^{*m}}{\sqrt{m!}}\left\langle n|m\right\rangle\right| \\ &= \left|e^{-\frac{\left(|\alpha_1|^2+|\alpha_2|^2-2\alpha_1\alpha_2^*\right)}{2}}\right| \\ &= e^{-|\alpha_1-\alpha_2|}\end{aligned} \tag{5.27}$$

Because of the non-commutativity of the non-orthogonal state projective measurement, a simple Von Neumann projective measurement cannot conclusively distinguish the different states.

For the sake of concision, we will only consider here the case of binary phase-shift keying (BPSK) in which 2 equally probable modulated binary symbols (0, 1) are represented by 2 antipodal phase states (0, π). This corresponds to a simple constant envelope modulation, in which the antipodal signals maximize the signal distance, and therefore minimize the overlap. As well the average received power is the same when the symbol 1 or 0 is transmitted.

In BPSK encoding, the two signal coherent states are devoted as $\left|\alpha_1\right\rangle = \left|\alpha\right\rangle$ and $\left|\alpha_2\right\rangle = -\left|\alpha\right\rangle$; the average signal photon number is $N_S = |\alpha|$, and the signal square overlap is:

$$\left|\langle \alpha_1 | \alpha_2 \rangle\right|^2 = e^{-2|\alpha_1 - \alpha_2|} = e^{-4N_S} \tag{5.28}$$

Assuming equally probable prior states: $\xi_0 = \xi_1 = 0.5$, the probability of error is finally the binary coherent Helstrom bound, corresponding to an ideal Dolinar receiver structure

$$BER = \frac{1}{2}\left\{1 - \sqrt{1 - \exp(-4N_s)}\right\} \tag{5.29}$$

Ban, Kurokawa, Momose and Hirota [17], based on the Bayes strategy, have also studied the problem of discrimination among symmetrical quantum states, arriving at the same bound for coherent states. They also consider the case of quantum estimation, which is important when the state includes unknown parameters, finding that the corresponding optimum estimation of POVM possesses a similar structure as those used for data detection. Furthermore, the asymptotical solutions for error probability and mutual information using higher order PSK and QAM constellation formats have been derived by Kato, Osaki, Sasaki and Omura [18].

The POVM is a generalization of a Von Neuman projection value measurement (PVM) of a signal observable, by projections onto orthogonal states, as discussed by Huttner, Muller, Gautier, Zbinden and Gisin [19], leading to conclusive results, but with finite error probability. The projection operators correspond to the standard (classical) receivers, e.g. heterodyne, homodyne, etc., for different signal observables: complex amplitude, signal quadrature, respectively; and even an optical Costas loop based on homodyne (Momose, Osaki, Ban, Sasaki and Hirota) [20]. Therefore their ultimate probability of error corresponds to the standard quantum limit (SQL). For homodyne detection of binary symmetric states we have [21]:

$$BER = \frac{1}{2} erfc\left(\sqrt{2N_S}\right) \tag{5.30}$$

where $erfc[x] = \left(2/\sqrt{\pi}\right)\int_x^{\infty} \exp(-t^2)dt$ is the complementary error function, where we use the notation of Sasaki, Usuda, and Hirota [22].

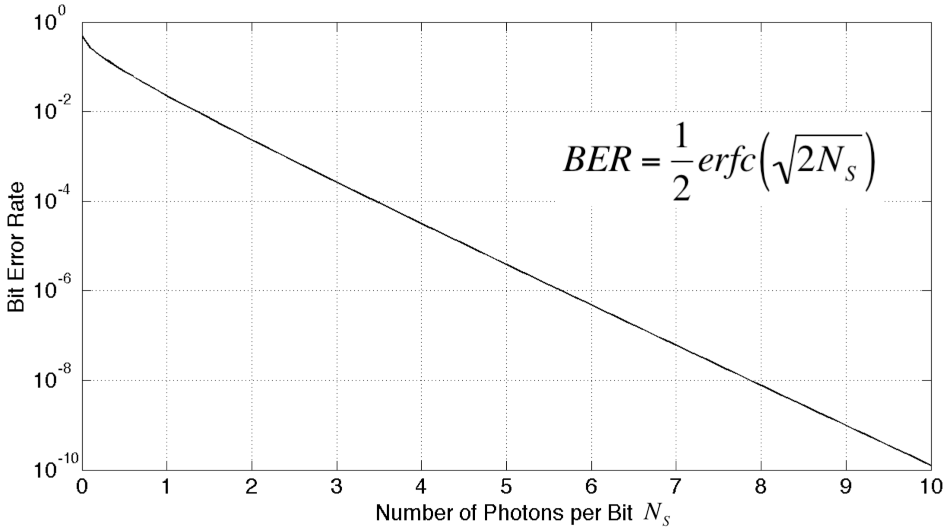


Figure 5.8 Homodyne detection BPSK bit error rate

As we have mentioned in 5.5 and (5.29), (5.30), the POVM measurement can provide superior performance than the classical receivers; however not only their physical implementation faces considerable challenges, but even its physical interpretation is a subject of research: Osaki, Ban and Hirota [23] have derived and interpreted the optimum detection operators for binary, ternary and quaternary optical phase-shift-keying modulated fields, based on the minimum probability of error criterion: they interpret the beating of the SQL as a “quantum interference” phenomenon.

While the POVM gives the probabilities of measurement of a quantum state, no indication about the structure of the physical device is in general suggested; Myers and Brandt [24], Banaszek [25] and Brandt [26] have investigated how to mechanize a photonic implementation of a POVM with applications to quantum information processing and quantum cryptography. As the optimal structures are difficult to mechanize, a practical detector must trade off the optimal performance and physical implementability. In the following sections we will only consider the SQL as in (5.30).

5.7 QPSK ENCODING FOR BB84 PROTOCOL

Phase encoding systems using homodyne detection are a promising technique for BB84 protocol by allowing at the same time a good approach to the quantum noise limited sensitivity and excellent spectral efficiency. The price to pay is obviously the availability of a strong phase reference at the receiver.

In BB84 protocol, from two orthogonal bases chosen randomly by Alice, four quantum eigen-states can be generated separately (the symbols 0 and 1 on two different bases $\{|\alpha\rangle,-|\alpha\rangle\}$ and $\{|i\alpha\rangle,-|i\alpha\rangle\}$), constituting a QPSK type constellation. After the random base switching at the receiver Bob's end, the states of base coincidence turn to a BPSK constellation whereas the states of base anti-coincidence are discarded and do not contribute to the shared information and therefore not to the BER. Alice's choices of bases and symbols and Bob's choices of bases, as well as the key coincidence/anti-coincidence are shown in Table 5-1.

Table 5-1 QPSK BB84 protocol

Alice					**Bob**			
Base	Bit	Φ_1	Φ_2	Φ_A	**Base**	Φ_B	Φ_A-Φ_B	Key
A1	0	0	$\pi/2$	$\pi/4$	**B1**	$\pi/4$	0	0
					B2	$-\pi/4$	$\pi/2$	?
	1	π	$-\pi/2$	$-3\pi/4$	**B1**	$\pi/4$	π	1
					B2	$-\pi/4$	$-\pi/2$	?
A2	0	0	$-\pi/2$	$-\pi/4$	**B1**	$\pi/4$	$-\pi/2$	?
					B2	$-\pi/4$	0	0
	1	π	$\pi/2$	$3\pi/4$	**B1**	$\pi/4$	$\pi/2$	?
					B2	$-\pi/4$	π	1

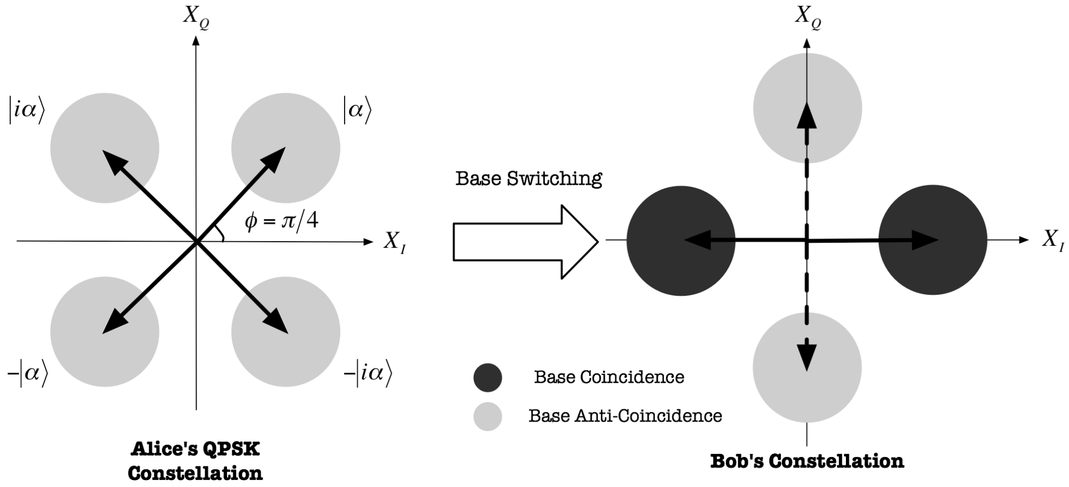


Figure 5.9 QPSK to BPSK conversion

REFERENCES

1. W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik”, *Zeitschrift für Physik* **43,** 172-198 (1927). English translation: J. A. Wheeler and H. Zurek, “The more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa”, *Quantum Theory and Measurement*, 62--84 (Princeton University Press 1983).
2. W. Heisenberg, *Die Physikalischen Prinzipien der Quantenmechanik (Leipzig: Hirzel)*, English translation “*The Physical Principles of Quantum Theory*” (Chicago: University of Chicago Press, 1930).
3. M. Fox, *Quantum Optics. An introduction* chapter 7, (Oxford University Press, 2006).
4. D. J. Griffiths, *Introduction to Quantum Mechanics*, (2nd ed. Prentice Hall 2004).

5. E. Schrödinger, “An undulatory theory of the mechanics of atoms and molecules”, *Physical Review* **28,** 1049--1070 (1926).

6. R. J. Glauber, “Coherent and incoherent states of the radiation field”, *Physical Review* **131**, 2766--2788 (1963).

7. J. R. Klauder, and B. Skagerstam, *Coherent States*, (World Scientific Pub Co Inc, Singapore, 1985).

8. P. Gallion, F.J. Mendieta, and S. Jiang, “Signal and quantum noise in optical communcation and in cryptography”. Elsevier 2008, to be published in *Progress in Optics* **52** (2008).

9. P. Carruthers, and M. M. Nieto, “Coherent states and the number-phase uncertainty relation”, *Physical Review Letters* **14**, 387--389 (1965).

10. R. Jackiw, “Minimum uncertainty product, number-phase uncertainty product, and coherent states”, *Journal of Mathematical Physics* **9**, 339--346 (1968).

11. M. Beck, D. T. Smithey, J. Cooper, and M. G. Raymer, “Experimental determination of number - phase uncertainty relations”, *Optics Letters* **18**, 1259--1261 (1993).

12. C. W. Helstrom, *Quantum Detection and Estimation Theory*, (Academic Press, New York 1976).

13. H. P. Yuen, R. S. Kennedy, and M. Lax, “On optimal quantum receivers for digital signal detection”, *Proceedings IEEE* **58**, 1170--1173 (1970).

14. O. Hirota, and H. Tsushima, “Quantum Communication Theory and Its Applications”, *The Transactions of the IEICE* **E72**, 460--470 (1989).

15. B. P. Belavkin, “Optimum distinction of non-orthogonal quantum signals”, *Radio Engineering and Electronics Physics* **20**, 39--47 (1975).

16. C. W. Helstrom, *Quantum Detection and Estimation Theory, Mathematics in science and Engineering* **123**, (Academic Press, New York 1976).

17. M. Ban, K. Kurokawa, R. Momose, and H. Hirota, “Optimum measurements for discrimination among symmetrical quantum states and parameter estimation”, *International Journal of Theoretical Physics* **36**, 1269--1287 (1997).

18. K. Kato, M. Osaki, M. Sasaki and O. Hirota, “Quantum detection and mutual information for QAM and PSK signals”, *IEEE Transactions on Communications* **4**, 248--254 (1999).

19. B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, “Unambiguous quantum measurement of nonorthogonal states”, *Physical Review A* **54**, 3783--3789 (1996).

20. R. Momose, M. Osaki, M. Ban, M. Sasaki, and O. Hirota, “On a relation between quantum interference and standard quantum limit”, *Proceedings of the 4th International Conference on Squeezed States and Uncertainty Relations*, *SPIE* **3322**, 307--312 (1996).

21. P. Agrawal, *Fiber-Optic Communication Systems*, chapter 10, (3rd edition Wiley-Interscience 2002).

22. M. Sasaki, T. S. Usuda and O. Hirota, “Physical aspect of the improvement of quantum noise characteristics caused by unitary transformation with a nonlinear optical medium”, *Physical Review A* **51**, 1702--1705 (1995).

23. M. Osaki, M. Ban, and O. Hirota, “Derivation and physical interpretation of the optimum detection operators for coherent-state signals”, *Physical Review A* **54**, 1691--1701 (1996).

24. J. M. Myers, H. E. Brandt, “Converting a positive operator valued measure to a design for a measuring instrument on the laboratory bench”, *Measurements Science and Technology* **8**, 1222--1227 (1997).

25. K. Banaszek, “Optimal receiver for quantum cryptography with two coherent states”, *Physics Letters A* **253**, 12--15 (1999).

26. H. E. Brandt, “Quantum measurement with a positive operator - valued measure”, *Journal of Optics B, Quantum and Semiclassical Optics* **5**, 266--270 (2003).

CHAPTER 6 TWO FIBER FIST IMPLEMENTATION OF A QPSK QUANTUM KEY DISTRIBUTION SYSTEM

In this chapter we first present a preliminary setup of a quantum key distribution system using QPSK modulations, then we introduce the main components in such a system and their characteristics. We also introduce the experimental techniques to overcome the system impairments such as polarization mismatch and phase drift.

6.1 DESCRIPTION OF THE TWO FIBER OPTICAL QPSK SYSTEM

Based on the BB84 protocol, in a phase encoding quantum key distribution system we use quadrature-phase-shift-keying modulation.

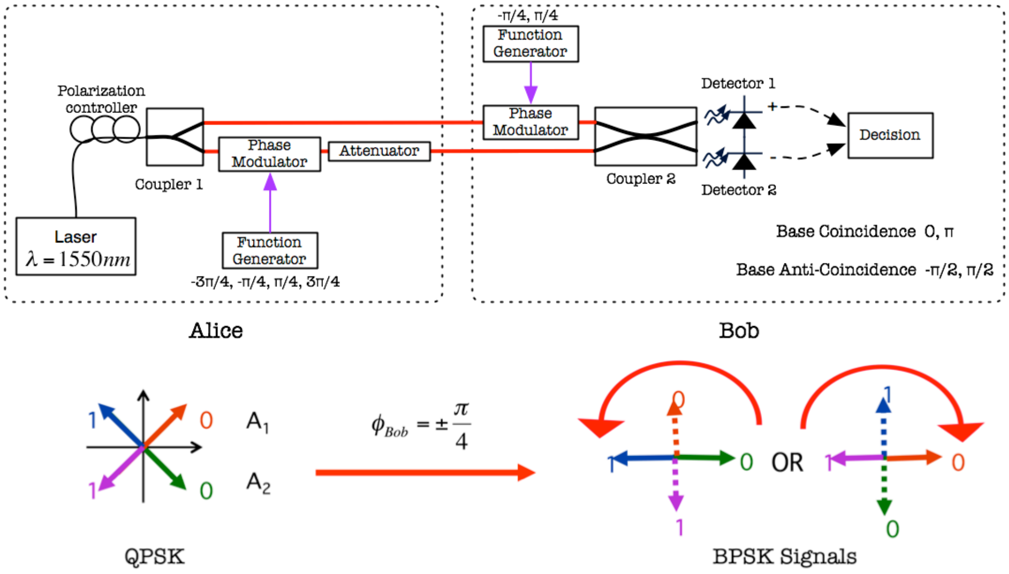


Figure 6.1 General representations of an optical QPSK modulation system using balanced homodyne detection

This is a general QKD arrangement using QPSK modulation. At the sender Alice's end, an optical coupler first separates the lightwave generated by the coherent laser source, directing to two outputs. On the lower arm, a function generator (FG) helps generate QPSK signal through an optical phase modulator according to Alice's base and symbol choices. At the receiver Bob's end, he introduces the base choice by applying π/4 or –π/4 phase shift on the upper arm phase modulator. A balanced configuration is used for the detection part. The QPSK modulated signals are converted to a BPSK signals since only one quadrature of the signal field is measured. We will introduce in the follow sections the other components used in the arrangement.

6.2 COMPONENTS IN A QPSK QKD SYSTEM

In order to move from the promise of theoretical physical laws to the hard reality of the electrical engineering world and to handle the quantum nature of light, in this section we introduce the main components that we have used for a quantum key distribution system implementation using QPSK BB84 protocol.

6.2.1 Laser Source

We use in our experiments an Integrated Laser electro-absorption Modulator (ILM) which combines a distributed feed back (DFB) laser diode with an integrated electro-absorption modulator on a single InP based chip. This laser source has been provided by gratefully by Jean-René Buric from Avanex.

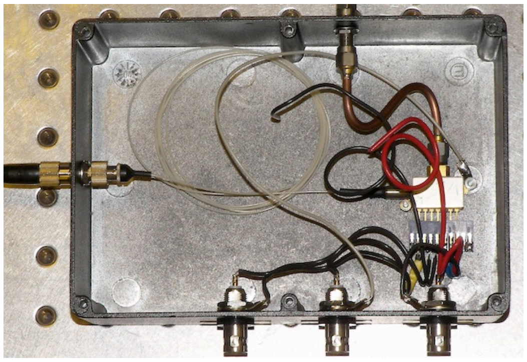
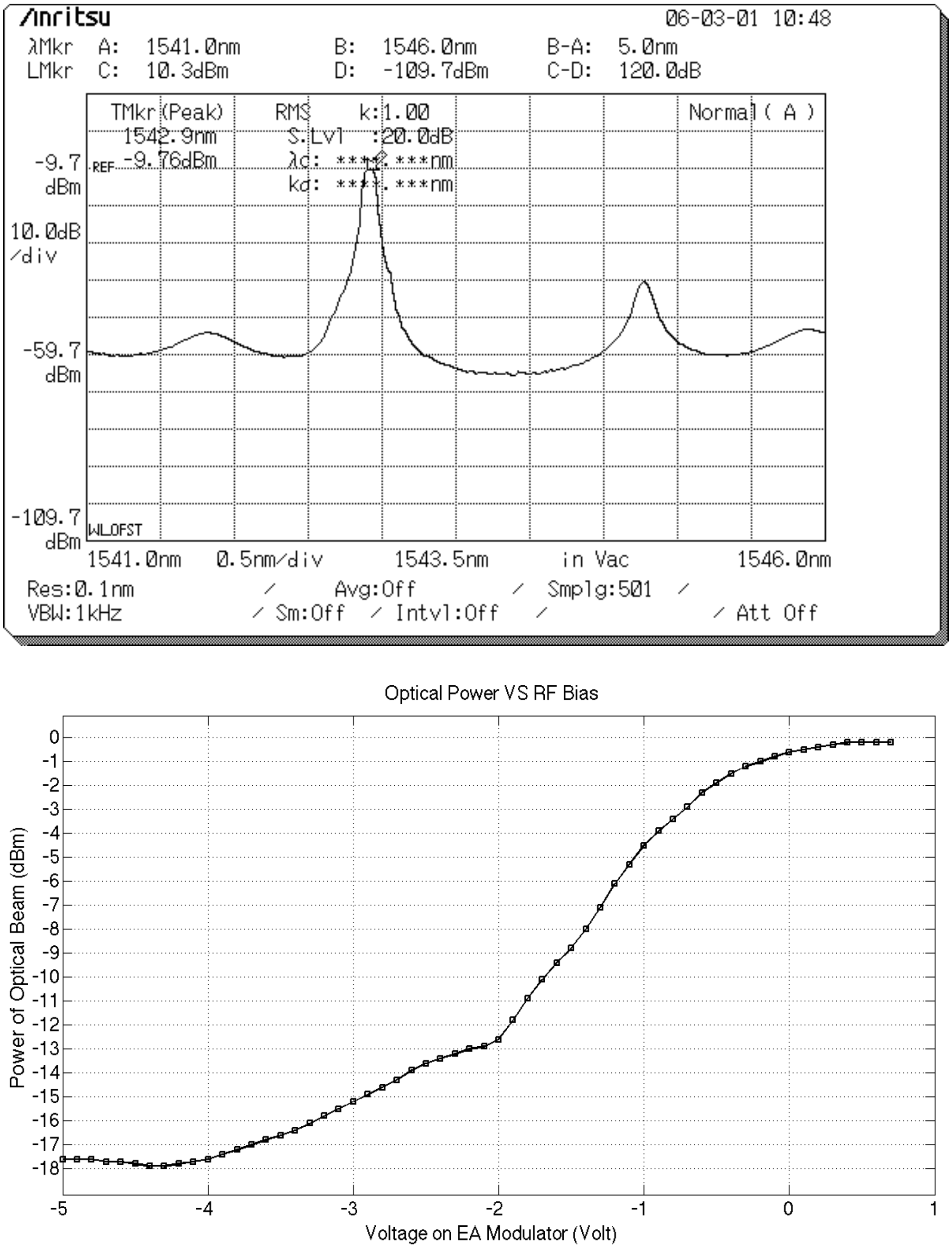


Figure 6.2 Avanex ILM module in the metallic box

The laser has been encapsulated in a metallic box as protection and helps dissipate the heat of laser. Three pins (Thermistor, TEC, Laser) are connected to SMA connectors (on the bottom) that control the laser operating temperature through thermistor resistance, thermoelectric cooler (TEC). The injected current adds a DC bias on the DFB laser.

The characteristics of the laser source are identical to those of *Avanex PowerSource 1915 LMM* module that allows 10 Gb/s data transmission [1,2], except for the extinction ratio. We have obtained the best optical extinction ratio at the wavelength 1542.9 nm, i.e. the maximum optical intensity ratio of the main lobe to the secondary lobe, by setting the operating temperature at 18 ºC with injected current at 33 mA.

The spectral line-width of the laser source as shown in Figure 6.3 a) is 0.05 nm, as the coherence time $\tau_c \approx \frac{1}{\Delta\omega}$ [3] is proportional to the range of angular frequencies, thus the coherent time is $\tau_c \approx 2.5 \times 10^{-11}\, s$, and the corresponding coherent length $L_c = c \cdot \tau_c \approx 0.01\, m$. The coherence time gives the time duration over which the phase of the light-wave train maintains consistent interference.



```
/inritsu                                                 06-03-01 10:48
λMkr  A:   1541.0nm         B:   1546.0nm      B-A:   5.0nm
LMkr  C:   10.3dBm          D:   -109.7dBm     C-D:   120.0dB
        TMkr (Peak)     RMS      k:1.00                Normal ( A )
          1542.9nm        S.Lvl   :20.0dB
 -9.7 REF -9.76dBm        λc:  ****.***nm
  dBm                     kσ:  ****.***nm
10.0dB
/div
-59.7
  dBm
-109.7 WLOFST
  dBm
      1541.0nm   0.5nm/div      1543.5nm      in Vac         1546.0nm
 Res:0.1nm            /      Avg:Off        /  Smplg:501  /
 VBW:1kHz            / Sm:Off  / Intvl:Off   /                 / Att Off
```

Figure 6.3 AVANEX ILM laser a) wavelength spectrum; b) optical power VS RF bias

The integrated intensity modulator has an input impedance at 50 Ω and is transparent without external modulation. The highest extinction ratio is 18 dB and can be obtained by applying -4.5 V to 0 V RF reverse voltage, as we show in Figure 6.3 b).

Table 6-1 Optimal operating parameters

Parameter	Value
Injected current	33 mA
Intensity Extinction	-18 dB
External Modulation	-4.5 Volts – 0 Volt
Temperature	18 ºC
Wavelength	1542.9 nm

6.2.2 Optical Coupler

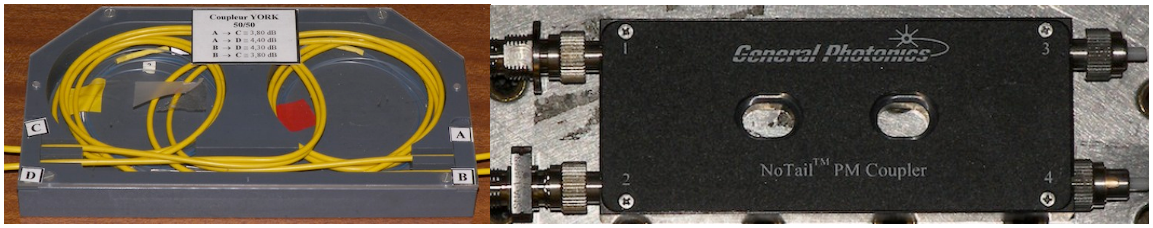


Figure 6.4 SMF 2×2 coupler and PM-NoTail 2×2 coupler

We have already given the physical and functional descriptions in chapter 4.4.1. In the QKD system setup we use single mode fiber (SMF) coupler and SMF polarization-maintaining (PM) coupler in our experiments, as illustrated in Figure 6.4.

6.2.3 Polarization Beam Splitter/Combiner

Polarization beam splitter or combiner (PBS/PBC) is a special optical 1×2 or 2×1 coupler that can be used either to combine light beams from two polarization-maintain input fibers into a single output fiber, or to split light from an input fiber into two output fibers of orthogonal polarization states. The PBS/PBC we use have a polarization extinction ratio at 25 dB, and the insertion loss around 0.5 dB.

We have used PBS and PBC in the Mach-Zender interferometers so as to reach a high polarization extinction ratio and to maintain the polarizations states since the modulators are also phase-sensitive.

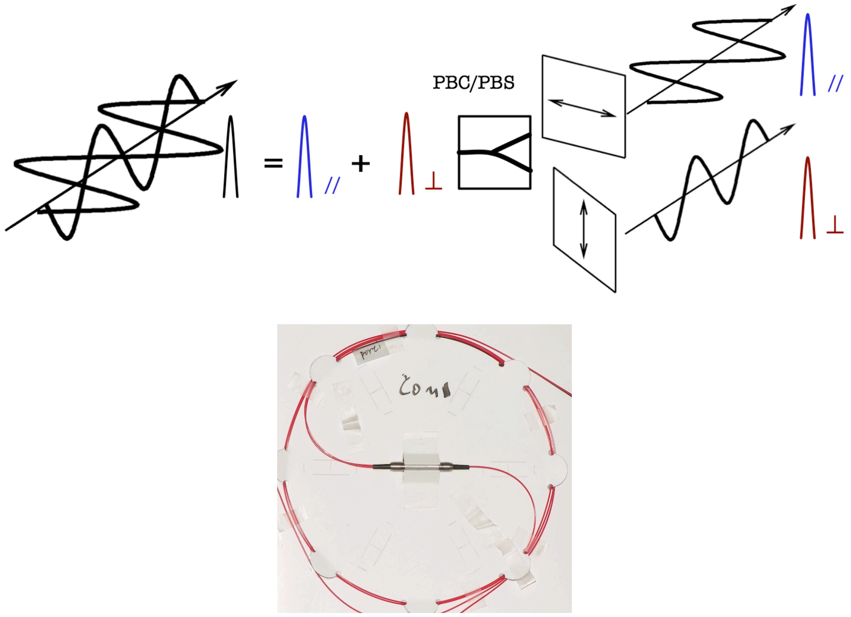


Figure 6.5 Polarization beam splitter/combiner

6.2.4 Polarization Rotator

Polarization rotators are used to manipulate and control the state of polarization (SOP) of an input beam of light and couple the adjusted light into an output fiber. They typically consist of an input with fiber pigtail or connector receptacle, from 1 to 3 polarization optic components and an output coupler with fiber pigtail, or connector receptacle. We use polarization rotator (OZ optics, 50 dB back reflection level) to maintain a linear polarization states in a desired axis.

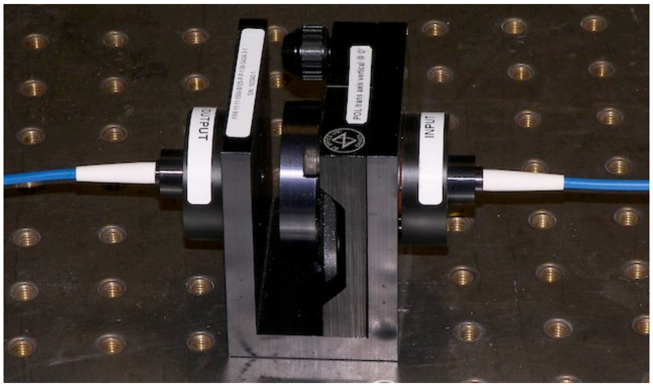


Figure 6.6 Polarization rotator

6.2.5 Polarization Controller

The principle of optic-fiber polarization controller is to use birefrigent components that introduce optical path differences of $\lambda/2$ or $\lambda/4$ between two main polarization axes. The $\lambda/4$ plate allows to convert a linear polarization into a circular or elliptical polarization, or to convert a circular or elliptical polarization into a linear polarization. The $\lambda/2$ plate introduces the rotation of polarization. A polarization controller usually consists of, two $\lambda/4$ plates on each side, i.e. the input and output side, and a $\lambda/2$ in the middle to rotate the polarization. Thus an arbitrary polarization output is attainable regardless of the input polarization. We use polarization controller to transfer circular or elliptical polarization into linear polarization states.

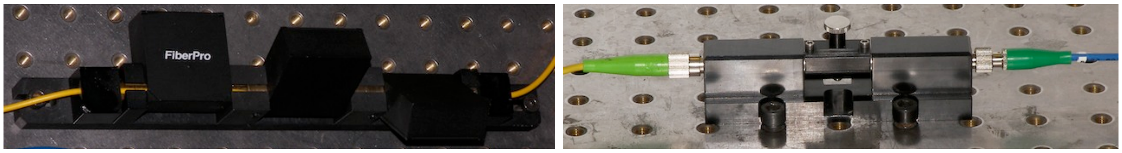


Figure 6.7 Pigtails connector and No-tail polarization controller

We have used single mode fiber (SMF) polarization controller and SMF polarization maintain (PM) coupler in our experiments, as illustrated in Figure 6.7, to adjust the lightwave polarization states before entering into the Mach-Zehnder interferometers at both Alice’s and Bob’s ends.

6.2.6 Optical Attenuator

Optical attenuator is used to generate “quantum level” signal in the quantum key distribution applications. As polarization mismatch is a main impairment in detection performance, we chose to use in-line variable attenuator using the “blocking technique” with polarization maintain optical fibers (polarization extinction ratio > 25dB).

In the blocking type attenuator, light from the source fiber is collimated into a beam approximately 0.4mm – 0.6mm wide. An adjustable blocking device is then inserted into the beam of collimated light in varying degrees depending on the attenuation required.

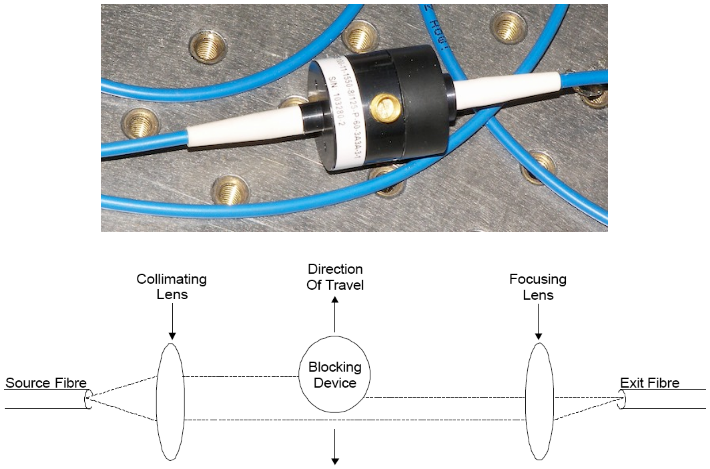


Figure 6.8 In-line variable optical attenuator using “blocking technique”

6.2.6 Mach-Zender Modulator using Double Electrodes

The phase modulation is one of the key functions in implementing a quantum cryptography protocol. As we have mentioned in BB84 QPSK protocol we need to constitute a four phase-state constellation to represent four symbols in two orthogonal bases, with two symbols in each base.

For the preliminary testing we have used $LiNbO_3$ Mach-Zender (MZ) intensity modulator with double electrodes at the sender Alice’s end to generate QPSK signals as it allows independent symbol and base choice. As we show in Figure 6.9, the structure of a

MZ modulator consists of a 1×2 waveguide coupler at the input, a 2×1 coupler at the output, as well as two electrodes on which we can apply electrical signals. At the receiver Bob's end we have used a same model $LiNbO_3$ intensity modulator to generate the BPSK signal according to the base choice.

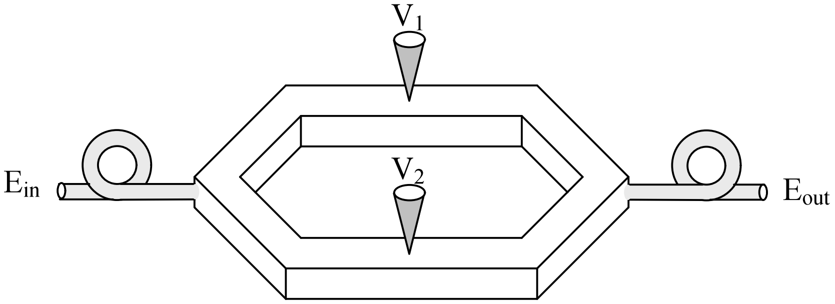


Figure 6.9 Structure of a Mach-Zender intensity modulator with double electrodes

The input optical signal enters the modulator via a polarization-maintaining optical fiber, and then a first Y-junction separates the input beam for transmission into two waveguides, called the upper arm and the lower arm. The distance between two arms is large enough so that the evanescent waves are negligible.

The refractive index of the electro-optic material is changed by an external tension, resulting in a phase difference between the two optical beams. The second Y-junction combines the two beams that interfere.

The phase difference between the two beams can be introduced in three ways:

- Applying an electric field on the electrodes of a single arm ($V_1 = 0$ or $V_2 = 0$);
- Applying an electric field on the arm of the two electrodes using the "push-pull" process ($V_1 = -V_2$);
- Applying different electric fields on both two arms to generate an arbitrary phase.

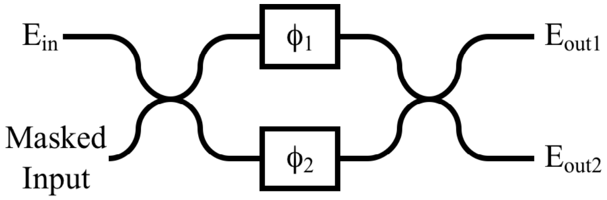


Figure 6.10 Phase modulation of Mach-Zender modulator

The relationships of the input and output are given by:

$$\begin{pmatrix} E_{out1}(t) \\ E_{out2}(t) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \cdot \begin{pmatrix} \exp j\phi_1 & 0 \\ 0 & \exp j\phi_2 \end{pmatrix} \cdot \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix}\begin{pmatrix} E_{in}(t) \\ 0 \end{pmatrix} \tag{6.7}$$

Thus the two outputs $E_{out1}(t)$ and $E_{out2}(t)$ can be represented by

$$\begin{cases} E_{out1}(t) = jE_{in}(t) \cdot \sin\left(\frac{\phi_1 - \phi_2}{2}\right)\exp j\left(\frac{\phi_1 + \phi_2}{2}\right) \\ E_{out2}(t) = -jE_{in}(t) \cdot \cos\left(\frac{\phi_1 - \phi_2}{2}\right)\exp j\left(\frac{\phi_1 + \phi_2}{2}\right) \end{cases} \tag{6.8}$$

Since the first terms of $E_{out1}(t)$ and $E_{out2}(t)$ are independent of the applied tensions, hence we can simplify the equations by replacing:

$$\begin{cases} \phi_1' = \phi_1 - \frac{\pi}{2} \\ \phi_2' = \phi_2 - \frac{\pi}{2} \end{cases} \tag{6.9}$$

Therefore the equation can be rewritten as:

$$\begin{cases} E_{out1}(t) = -E_{in}(t) \cdot \sin\left(\frac{\phi_1' - \phi_2'}{2}\right)\exp j\left(\frac{\phi'_1 + \phi_2'}{2}\right) \\ E_{out2}(t) = E_{in}(t) \cdot \cos\left(\frac{\phi_1' - \phi_2'}{2}\right)\exp j\left(\frac{\phi_1' + \phi_2'}{2}\right) \end{cases} \tag{6.10}$$

As we can see from Figure 6.11, only one output $E_{out2}(t)$ is used while the other is masked. If we maintain $\phi_1 - \phi_2 = \pm\frac{\pi}{2}$, then we can obtain

$$E_{out}(t) = \frac{\sqrt{2}}{2} E_{in}(t) \exp j\left(\frac{\phi_1 + \phi_2}{2}\right) = \frac{\sqrt{2}}{2} E_{in}(t) \exp j\left(\frac{\phi_{Alice}}{2}\right) \tag{6.11}$$

In Figure 6.11 we show the double-electrode MZ modulator used in our experiments. The tension V_π corresponds to the tension value that adds a phase variation π in the optical field. We have used two MZ modulators with high input resistance connector. The maximum input optical power is 10 mw and the maximum applied tension is ±15 V. The table below presents their characteristic values.

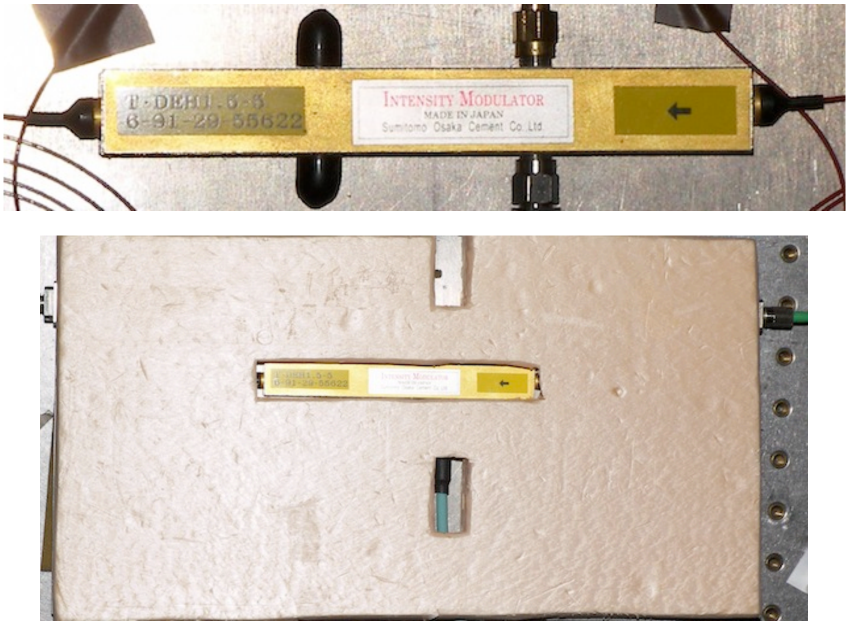


Figure 6.11 Mach-Zehnder intensity modulator using double-electrode and styrofoam thermal protection

The phase modulation on two electrodes can be obtained as:

$$\phi_1(t) = \frac{\pi \cdot \left(V_1(t) + V_{R1}\right)}{V_{\pi 1}} \tag{6.12}$$

$$\phi_2(t) = \frac{\pi \cdot \left(V_2(t) + V_{R2}\right)}{V_{\pi 2}} \tag{6.13}$$

where the $V_1(t)$ and $V_2(t)$ are the tensions applied on the electrode 1 and the electrode 2, $V_{\pi 1}$ and $V_{\pi 2}$ are the half-wave voltage, V_{R1} and V_{R2} are the residual tensions due to the dissymmetry between the two optical paths.

Table 6-2 Characteristics of Sumitomo Osaka MZ modulators

	MZ6-91-29-55-621		MZ6-91-29-55-622	
Insertion Loss (dB)	4.0		4.5	
	Electrode 1	Electrode 2	Electrode 1	Electrode 2
V_π (Volts)	3.6	3.6	3.6	3.6
Extinction Ratio (dB)	31.6	31.8	32.2	32.3
Bandwidth (GHz)	7.9	8.1	8.1	8.0

In the protocol BB84, we chose to use $\phi_1 - \phi_2 = \pm\frac{\pi}{2}$ so as to maintain a constant envelope and generate a QPSK constellation.

Table 6-3 Alice's QPSK constellation and Bob's BPSK modulation

Alice							**Bob**				
Base	**Bit**	$\mathbf{\Phi_1}$	**FG 1**	$\mathbf{\Phi_2}$	**FG 2**	$\mathbf{\Phi_A}$	**Base**	$\mathbf{\Phi_B}$	**FG 3**	$\mathbf{\Phi_A\text{-}\Phi_B}$	**Key**
A1	0	0	0 V	π/2	1.8 V	π/4	**B1**	π/4	1.8 V	0	0
							B2	-π/4	-1.8 V	π/2	?
	1	π	3.6 V	3π/2	5.4 V	-3π/4	**B1**	π/4	1.8 V	π	1
							B2	-π/4	-1.8 V	-π/2	?
A2	0	0	0 V	-π/2	-1.8 V	-π/4	**B1**	π/4	1.8 V	-π/2	?
							B2	-π/4	-1.8 V	0	0
	1	π	3.6 V	π/2	1.8 V	3π/4	**B1**	π/4	1.8 V	π/2	?
							B2	-π/4	-1.8 V	π	1

6.2.7 Phase Modulator

We have validated the preliminary system with the MZ modulators, however, the MZ modulators requires very precise voltage control since they are subject to both intensity and phase modulation, especially for QPSK modulations. Moreover, MZ modulators are usually not polarization-dependent, which induces additional difficulties for coherent homodyne receiver.

We have then improved the system setup by using Photline $LiNbO_3$ phase modulators MPZ-LN-10 and MPX-LN-0.1 to generate QPSK signals as well as for the base choice.

$LiNbO_3$ phase modulators are widely used for their high bandwidth performance that makes them favored devices for high data optical communications (up to 40 Gb/s) and high frequency (20 GHz) analog transmission. It can offer advantages of low optical losses, high extinction ratio. Z-cut $LiNbO_3$ phase modulator can provide lower driving voltage than X-cut $LiNbO_3$ phase modulator. The X-cut modulator MPX-LN-0.1 used in our setup is a specially designed phase modulator that limits the passband to 0.1 GHz and offers a much lower V_π at 3.4 Volts with high input impedance.

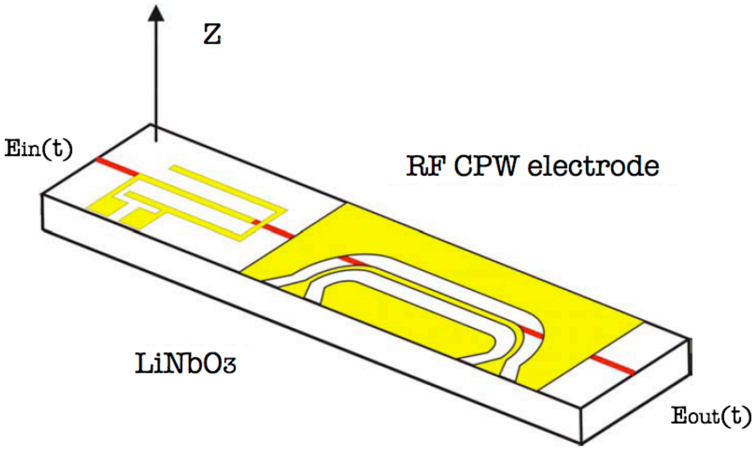


Figure 6.12 Physical structure of a phase modulator on a Z-cut $LiNbO_3$ crystal

An optical phase modulator can be obtained by diffusing an optical channel waveguide at the surface of a Z-cut Lithium Niobate crystal. The main direction of propagation can be oriented parallel to the X- or Y-axis. Cr-Au traveling wave electrodes are deposited over a thick dielectric buffer layer in order to prevent undesirable optical absorption of the TM-mode, and also in order to get the microwave to optical phase matching condition.

As a RF signal $S(t)$ is applied on the electrode, the phase variation $\phi(t)$ can be obtained at the output of the modulator illuminated by an optical beam polarized along the Z-axis, i.e., the TM polarization, with the effective half-wave voltage $V_{\pi}(\lambda,\omega_{RF})$ that is related to wavelength λ and RF frequency ω_{RF}. $\phi(t)$ can be given by:

$$\phi(t) = \frac{\pi}{V_{\pi}} S(t) \tag{6.14}$$

If the insert loss is L, then the output field can be represented by

$$E_{out}(t) = L \cdot E_{in}(t)\exp\big(j\phi(t)\big) \tag{6.15}$$

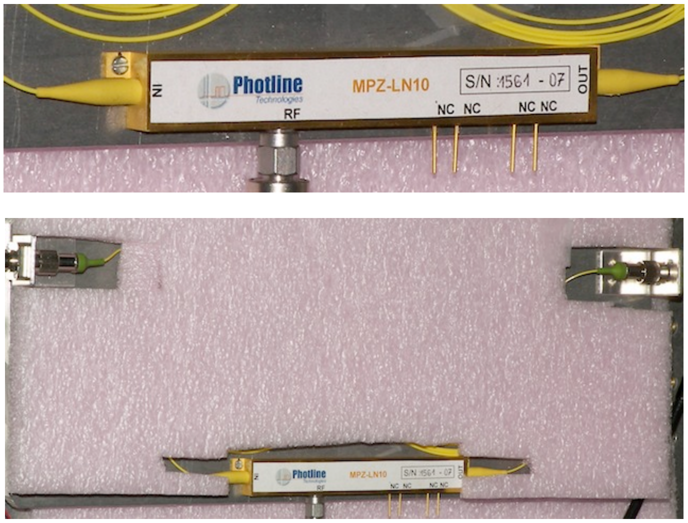


Figure 6.13 $LiNbO_3$ phase modulator and thermal protection

As the modulation is only operated on the TM polarization, polarization controller and polarization-maintaining fiber are required. As well, the input lightwave polarization must be aligned along Z-axis so as to maximize the polarization extinction ratio.

The specification of this phase modulator is shown in Table:

Table 6-4 Characteristics photline phase modulators

Serial Number	2354-13	1561-07
Product ID	MPX-LN-0.1	MPZ-LN-10
Insertion Loss (dB)	2.7	3.0
Polarization dependent Loss (dB)	4.3	1.0
Input resistance (Ω)	10000	50
Bandwidth (GHz) -3dB	0.1	10
V_π at 10 MHz (Volts)	3.4	6.0

6.2.8 Balanced Photo-Receiver

Balanced photo-detector subtracts two output signals from each other, resulting in the cancellation of common mode noise. This allows small changes on the signal to be extracted from the interfering noise floor. We chose InGaAs photodiodes with a switchable version (Thorlabs PDB150C-AC) with selectable transimpedance gain.

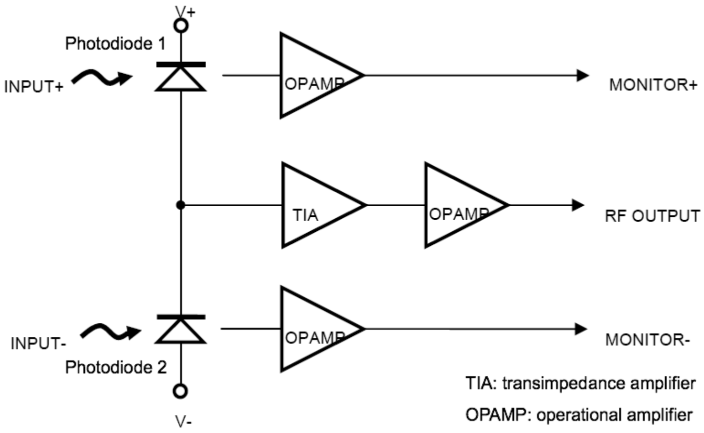


Figure 6.14 Functional block diagram

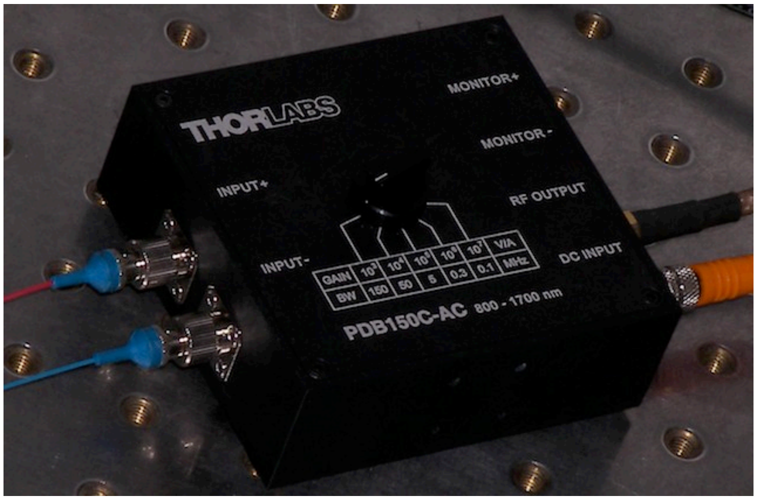


Figure 6.15 Balanced photodetectors (Thorlabs PDB150C-AC)

Table 6-5 Balanced photodetectors characteristics

	PDB150C-AC				
Wavelength Range	800 nm-1700 nm				
Typical Max. Responsivity	1.0 A/W				
Detector Diameter	0.3 mm				
Bandwidth -3dB (MHz)	150	50	5	0.3	0.1
Transimpedance Gain (V/A)	10^3	10^4	10^5	10^6	10^7
Conversion Gain RF (V/W)	10^3	10^4	10^5	10^6	10^7
Conversion Gain Monitor	10 V/mW @ 1550 nm				
CW Saturation Power	5 mW @ 1550 nm				
Max. Input Power	20 mW				
RF-Output Impedance	50 Ω				
Minimum NEP (DC-10 MHz)	0.3 pW/√Hz				
Power Supply	±12 V, 200 mA				

We have measured the noise level using bandwidth at 50 MHz using signal optical power of -50 dBm and LO optical power of -9 dBm.

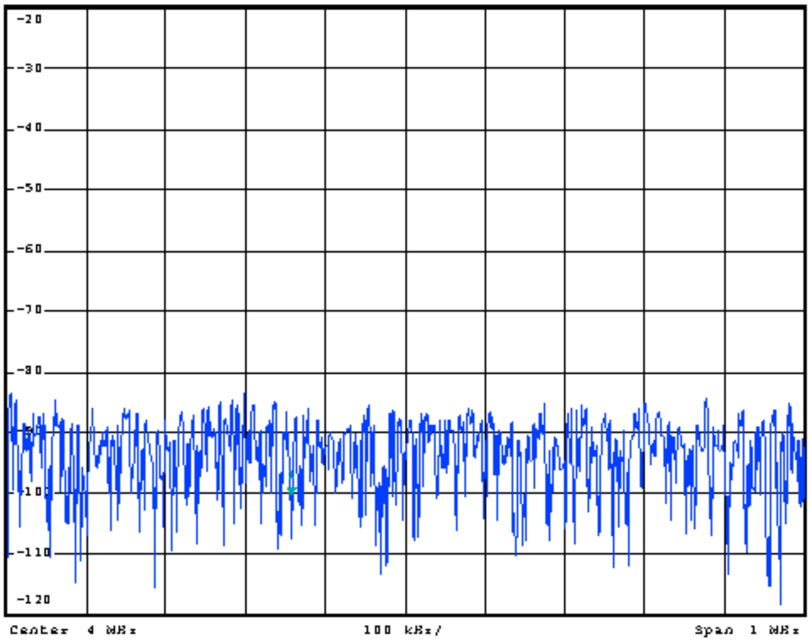


Figure 6.16 Noise measure with vacuum field, noise level ≈ -95 dBm

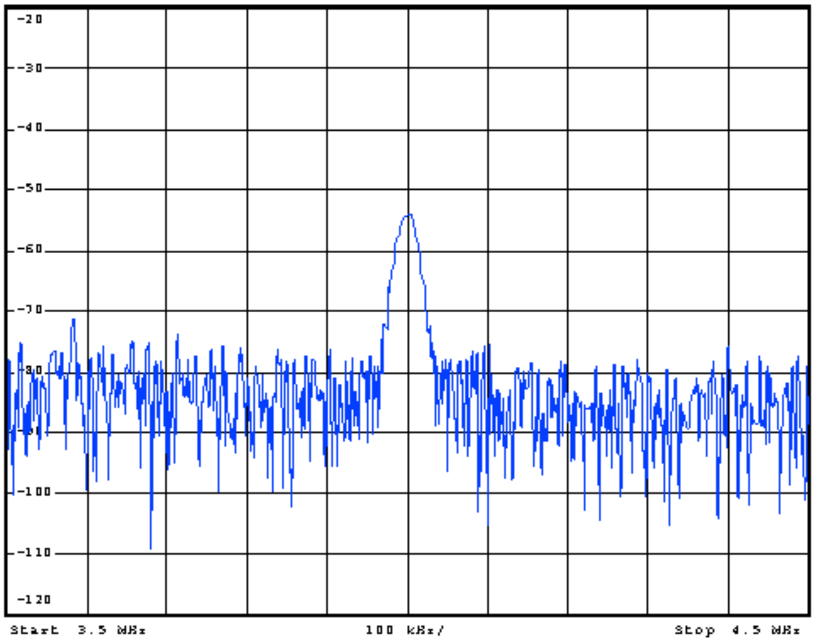


Figure 6.17 Single-port output, noise level ≈ -85 dBm, signal level ≈ -56 dBm

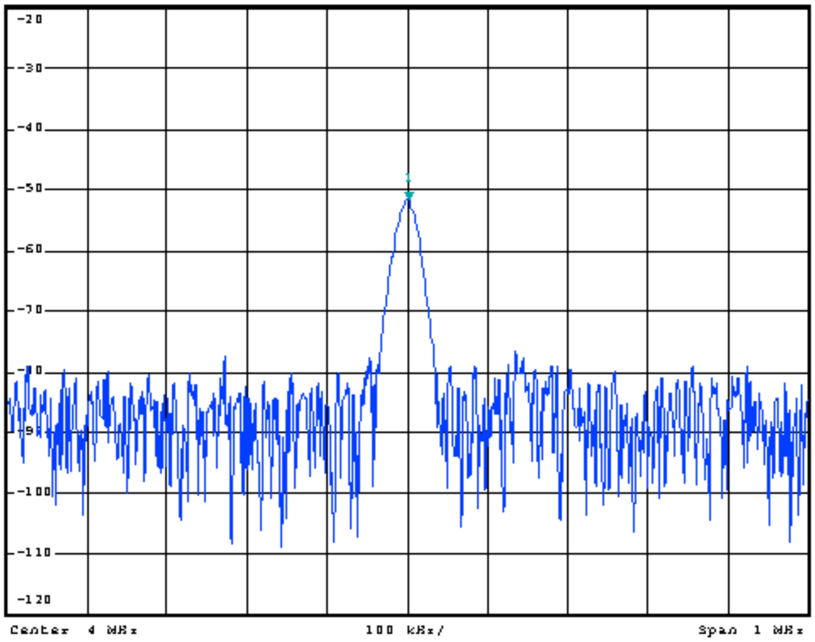


Figure 6.18 Balanced output, noise level ≈ -90 dBm, signal ≈ -51 dBm

In classical approach, from the above experimental results, we can see that the subtraction of the two currents provides the homodyne signal in which the DC term is eliminated during the subtraction process when the two branches are balanced in such a way that each branch receives equal signal and local-oscillator powers. More importantly, the intensity noise associated with the DC term is also eliminated during the subtraction process, because the same local oscillator provides power to each branch. As a result, intensity fluctuations in the two branches are correlated and cancel out during subtraction of the photocurrents. It should be noted that intensity fluctuations associated with the homodyne term couldn't be canceled even in a balanced receiver. As a result there is a residual noise on power difference, which can be shown to be equivalent to the shot noise of a beam of power sum, i.e. the LO and signal can be shot noise limited. However, their impact is less severe on the system performance because of the square-root dependence of the homodyne term on the LO power [4].

Balanced receivers have two advantages: first, the noise floor problem is overcome by using a strong LO. Second, all of the signal and LO power is used effectively. A single-port receiver such as that shown in Figure 6.17 would reject half of the signal power P_S (and half of LO power P_{LO}) during the mixing process. This power loss is equivalent to a 3-dB optical power penalty, or a 6-dB electric power penalty. Balanced receivers use all of the signal power and avoid this power penalty. At the same time, all of the LO power is used by the balanced receiver, making it easier to operate in the shot-noise limit.

6.3 SIGNAL DETECTION AND SYSTEM VALIDATION

Our first experiment to validate this QPSK BB84 implementation consists of a standard optical fiber self-homodyne system with a strong carrier “reference” transmitted in a separate optical line. The modulated signal arm was constructed to have the Modulator-Alice (MOD-A) followed by an optical attenuator; Bob introduces his base choices on the Modulator-Bob (MOD-B) in the lower reference arm at the reception, the setup is shown in Figure 6.19.

In this setup, we have used the two $LiNbO_3$ phase modulators: MPX-LN-0.1 is used as MOD-A since its low V_π facilitates the QPSK modulation and MPZ-LN-10 is used as MOD-B for the BPSK base switching.

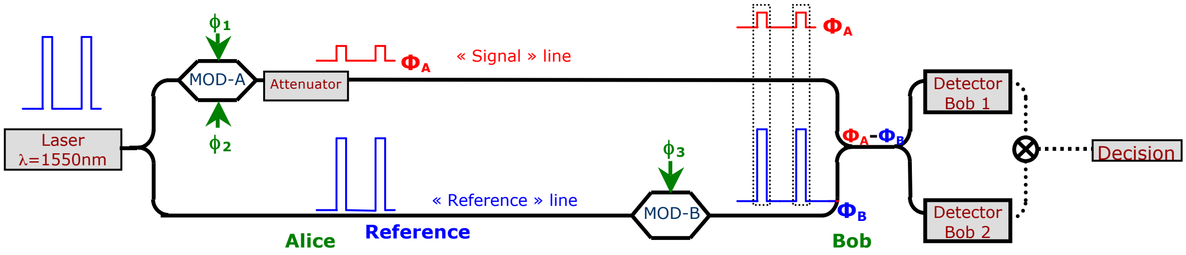


Figure 6.19 QPSK self-homodyne setup

In the Table 6-6 we show the modulation signals for the BB84 protocol. The curve in Figure 6.20 a) is the waveform of an oscilloscope screening of QPSK modulation signal generated by function generator 1 (FG 1); the curve in Figure 6.20 b) is the waveform BPSK modulation signal generated by FG 2. Actually we also apply a DC offset at the phase modulators so as to adjust the original phase state. The detected signals at Bob's end are shown in Figure 6.20 c). We obtain positive-valued pulses for the key bit 0, and negative-valued pulses for the key bit 1. When there are base anti-coincidences, we receive undistinguishable value "zero", and these bits will be discarded.

Table 6-6 QPSK BB84 modulation using phase modulators

Alice				**Bob**				
Base	**Bit**	**Φ_A**	**FG 1**	**Base**	**Φ_B**	**FG 2**	**Φ_A-Φ_B**	**Key**
A1	0	π/4	0 V	**B1**	π/4	3.0 V	0	0
				B2	-π/4	0 V	π/2	?
	1	-3π/4	-3.4 V	**B1**	π/4	3.0 V	π	1
				B2	-π/4	0 V	-π/2	?
A2	0	-π/4	-1.7 V	**B1**	π/4	3.0 V	-π/2	?
				B2	-π/4	0 V	0	0
	1	3π/4	1.7 V	**B1**	π/4	3.0 V	π/2	?
				B2	-π/4	0 V	π	1

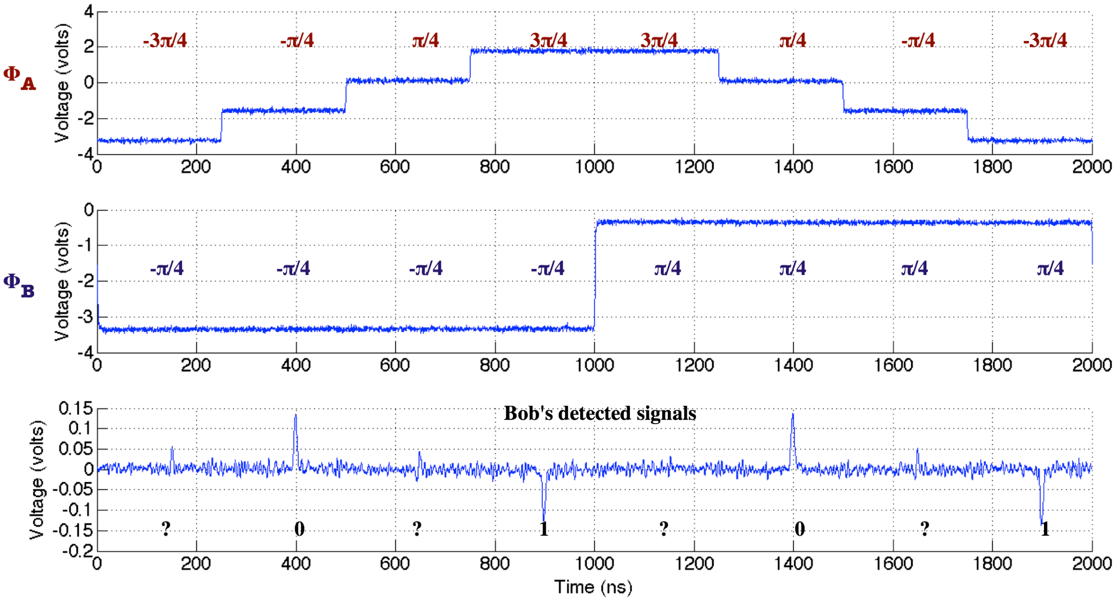


Figure 6.20 a) QPSK modulating signal of FG 1 with input load 10 kΩ; b) BPSK modulating signal of FG 2 with input load 50 Ω; c) Bob's detected signals with all the 8 possible combination as in Table 6.6

6.4 SYSTEM IMPAIRMENTS ANALYSIS

The homodyne receiver for QKD applications must be designed to compensate for the phase and polarization fluctuations in both interferometers and in the residual differential propagation channel characteristics.

6.4.1 POLARIZATION MISMATCH IMPAIRMENTS

The polarization state of the received optical signal plays no role in direct-detection receivers simply because the photocurrent generated in such receivers depends only on the number of incident photons. This is no more the case for the coherent receivers, whose operation requires matching the state of polarization of the local oscillator to that of the received signal. The polarization-matching requirement can be understood from the analysis of in Annex B, where the use of scalar fields E_S and E_{LO} implicitly assumed the same polarization state for the two optical fields by using polarization-maintain components, such as PM fiber, PBS/PBC, etc. The interference of E_S and E_{LO} is used by the decision circuit to reconstruct the transmitted bit stream, any change in polarization match reduces the signal and affects the receiver performance. In particular, if the polarization states of E_S and E_{LO} are orthogonal to each other, the signal disappears. Therefore any change in polarization affects the BER through changes in the receiver current and SNR.

6.4.2 Phase Drift in Mach-Zehnder Interferometers

The differential delay time between signal and reference pulses caused by the long and short arms of Alice's and Bob's interferometers should be kept stable so as to allow a continuous QKD operation [5,6]. Nevertheless the interferometers should be operative in different location; moreover they are subject to different temperature, pressure and mechanical stress conditions. As we have attested in the experiments, environmental variation could induce different phase variations in upper and lower arm of interferometers: a phase drift over 6π has been observed in our Mach-Zehnder interferometer setup over 16 hours, as show in Figure 6.21.

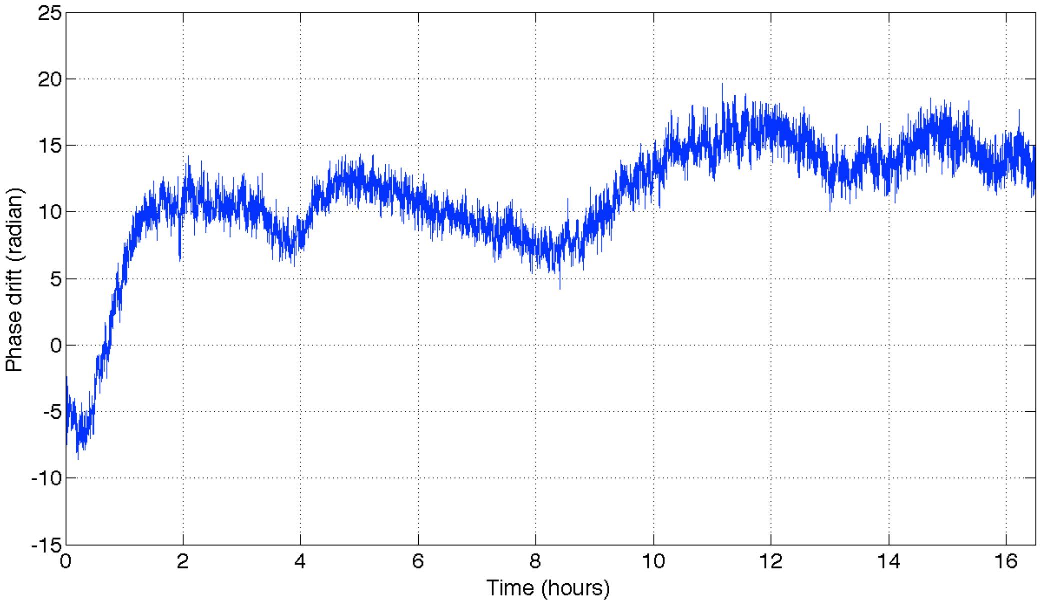


Figure 6.21 Mach-Zehnder interferometer phase drift

We assume the total phase shift at Bob's end is:

$$\Phi = \Phi_0 - \Delta\Phi \tag{6.16}$$

where $\Phi_0 = \Phi_{Alice} - \Phi_{Bob}$ and $\Delta\Phi$ is the system phase drift, i.e. the extraneous phase shift. To keep the system usable, the threshold of Quantum Bit Error Rate (QBER) is in the range of 11%, with a reduced key generation. This $QBER_{threshold}$ corresponds to phase error $\Delta\Phi \approx 27°$ [7-9].

6.5 TRAINING FRAME FOR PHASE DRIFT COMPENSATION

The real-time phase error compensation could be realized on Bob's interferometer by adding a fiber stretcher [7], or by phase adjustment on Bob's modulator [8]. The phase compensation algorithm is based on the QBER measurements, thus we insert the training frames into the key frames periodically to calculate the phase error and compensate the phase drift.

6.5.1 NUMERICAL RESULTS USING TRAINING FRAME

As the phase shift is a random process that is determined by many external variations, in our experiments we first fixed Φ_0 to measure the phase variation. Then post-detection phase tracking algorithm was carried out numerically by taking successively 20% and 5% of data transmission as training frames, as shown in Figure 6.22, Figure 6.23. We can see that the phase error $\Delta\Phi$ could both be well controlled within the range in the first two cases; however the trade-off is to be taken between QBER and training frames' payload. In fact the percentage of training frames could be adjusted according to the QKD link characteristics, such as the temperature variations, the detector efficiency, the interferometer visibility; it depends also on the higher-level key generation protocols such as privacy amplification [10].

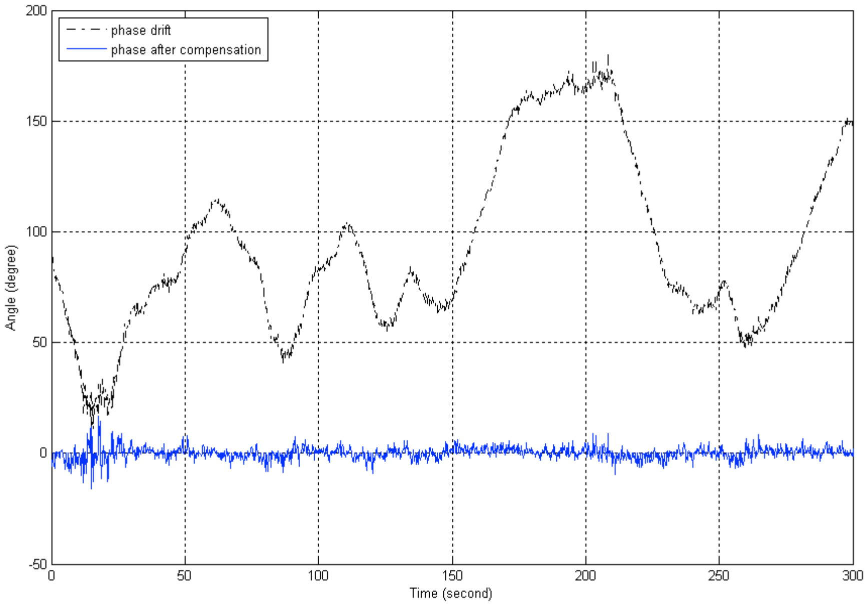


Figure 6.22 Phase compensation using 20% training frames: in this simulation the corrected phase error (the lower curve) is very small, thus a low QBER is obtained.

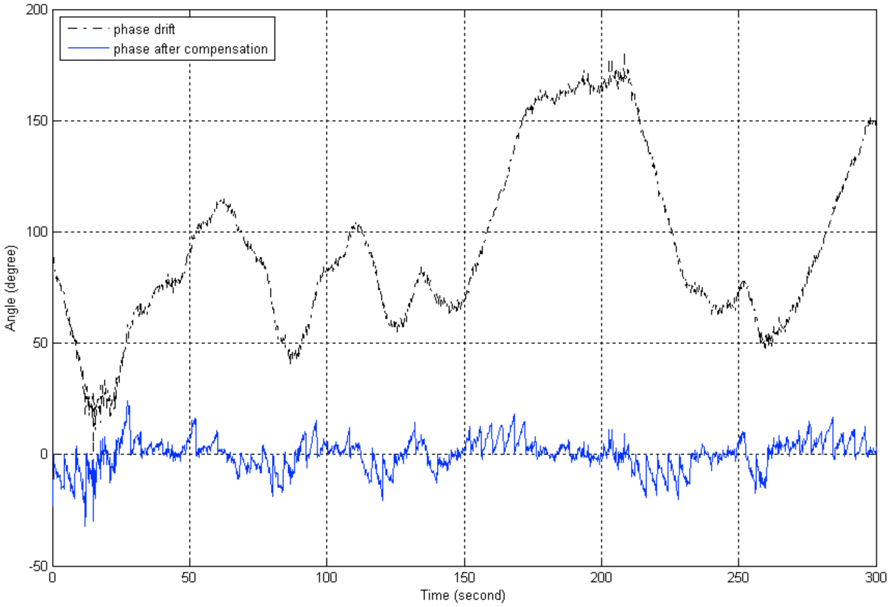


Figure 6.23 Phase compensation using 5% training frames: in this simulation the corrected phase error (the lower curve) is relatively higher, thus a higher QBER is obtained.

6.5.2 Criteria of Training Frames

The training frames contain predetermined Qbits sequence: Alice and Bob agree on the symbols and base choices prior to the transmission. The portion of training frames is directly related to the phase error tolerance: the weaker the signal pulses, the longer the training frame interval should be due to the bits erasure. Another reason is that provided the density of probability of the measured WCP follows Gaussian distribution with mean photon number N_S, the standard deviation is $\Delta N_S = N_S^{1/2}$. Additionally the Heisenberg energy-time uncertainty principle gives a lower bound on the product of the standard deviations $\Delta N_S \geq 1/2$ [11]. Therefore the training frames should contain a large number of samples so as to reach to a good precision for phase error measurements, and we use four registers R_0, $R_{\pi/2}$, R_{π}, $R_{3\pi/2}$ to store and update the estimated values for the four possible phase states [12,13].

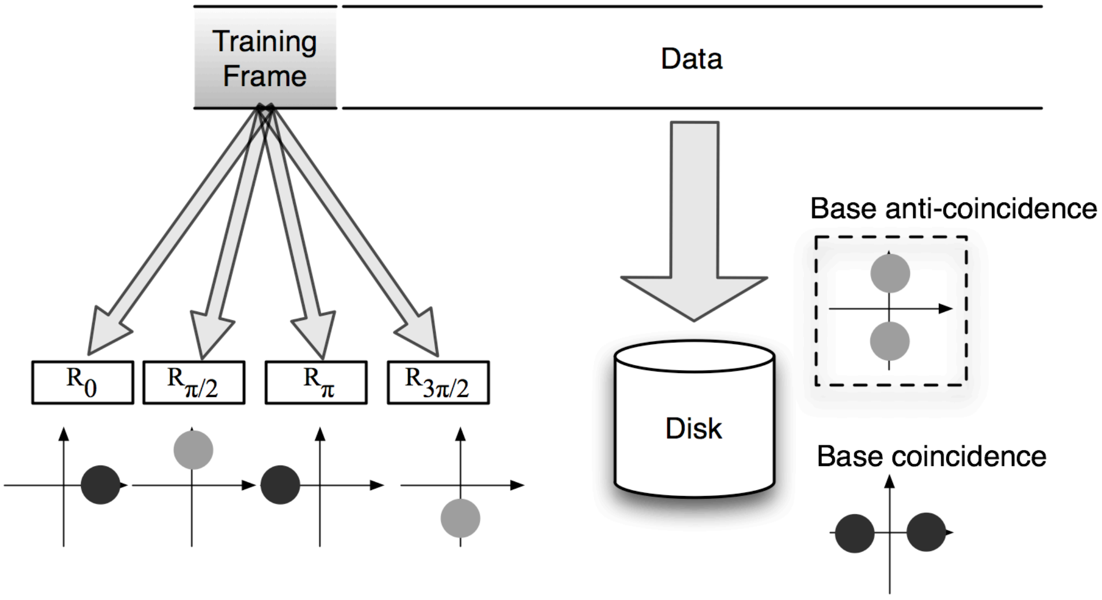


Figure 6.24 Training frames and data frames

If we consider the mean value $\mu = A$ and standard deviation σ, the individual outputs of the balanced receiver follow the Gaussian statistics. According to the central limit theorem, with M independent samples, we will obtain the normal distribution

$\mathrm{N}\left(\mu,\sigma/\sqrt{M}\right)$. If we want to have the uncertainty of amplitude estimation less than E, then the condition in the equation (6.17) must be met:

$$erfc\left(\sqrt{2M}/2\sigma\right) \approx \exp\left(-M/2\sigma^2\right) < E \tag{6.17}$$

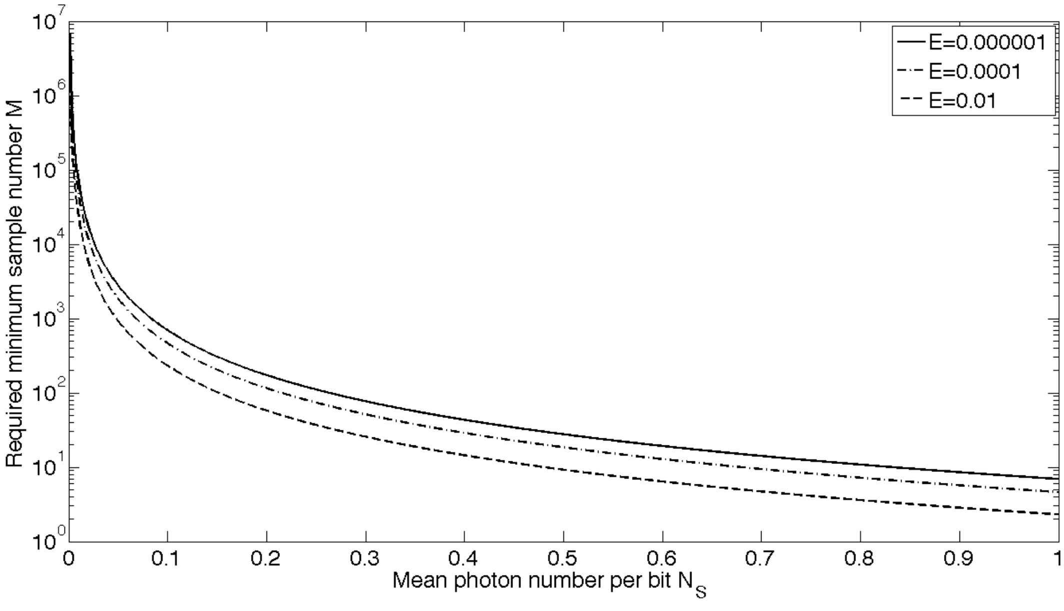


Figure 6.25 Minimum sample number M for corresponding mean photon number N_S

Now let us take a close look at the equation (6.17) and assume that the measurements are made for coherent states. For M samples with mean photon number N_S, the total photon number to determine the state value is:

$$N_{total} = N_S \cdot M \tag{6.18}$$

therefore the equation (6.17) turns into:

$$erfc\left(\sqrt{2M}/2\sigma\right) = erfc\left(\sqrt{2N_{total}/N_S}/2\sigma\right) < E \tag{6.19}$$

From equation (6.19) we can also deduce the following fact: if we repeatedly measure a weak coherent state with mean photon number N_S for M times in a classic bipolar BPSK coherent detection system and set “zero” as the threshold, and we take the mean value of these M samples as the bit value, the bit error rate R_E will be $E/2$ since only those falling into one side are considered as bit errors. Furthermore since the standard deviation of signal with mean photon number $N_S = 1$ corresponds to $1/2$ photon energy, we can normalize the output standard deviation by replacing $\sigma = \frac{1}{2\sqrt{N_S}}$, then we obtain:

$$R_E = \frac{1}{2} erfc\left(\sqrt{2N_{total}/N_S}/2\sigma\right) = \frac{1}{2} erfc\left(\sqrt{2N_{total}}\right) = \frac{1}{2} erfc\left(\sqrt{2M \cdot N_S}\right) \tag{6.20}$$

Compared with the classical homodyne detection performance equation of BER:

$$BER = \frac{1}{2} erfc\left(\sqrt{2N_S}\right) \tag{6.21}$$

Hence we can have a very interesting conclusion: using *M* samples of mean photon number N_S gives the same *BER* performance as using a single sample but with mean photon number of $M \cdot N_S$, as long as the laser source is perfectly coherent. High photon number involved during each observation time, i.e. the bit duration, in an optical communication system, or high sample number involved in weak coherent signal detection can both smooth out by ensemble averaging major aspects of the quantum nature of light.

6.5.3 Piezoelectric Phase Shifter and External Driver

The all fiber phase shifter (General photonics) provides convenient phase shift/modulation in a compact package. The insertion loss is less than 0.5 dB and permits a good precision of phase tuning.

The optical phase shift is achieved using an electrical driving signal. As $V_\pi = 9.95\ Volts$, we have to use an external driver that delivers at a dynamic range from -11 volts to 155 volts. The external driver allows a dynamic range [-8π, 8π] and a response time of few milliseconds. We use the phase shifter for the phase drift compensation based an opto-electric feedback loop.

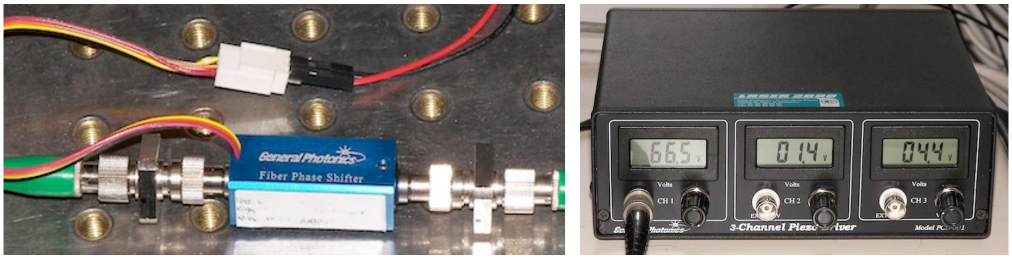


Figure 6.26 Phase shifter and external driver

REFERENCES

1. M. B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, and F. J. Mendieta, “Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol”, *Photonics North 2006*, *Proceeding of SPIE* **6343**, (2006).

2. Avanex Corporation, “PowerSourceTM 1915 LMM 10 Gb/s digital electro-absorption laser module - 1600 ps/nm”.

3. M. Fox, *Quantum Optics. An introduction* chapter 2.3, (Oxford University Press, 2006).

4. P. Agrawal, *Fiber-Optic Communication Systems*, chapter 10.4.2, (3rd edition Wiley-Interscience 2002).

5. K. Inoue, E. Waks, and Y. Yamamoto, “Differential-phase-shift quantum key distribution using coherent light”, *Physical Review A* **68**, 022317 (2003).

6. H. Takesue, S. W. Nam, Q. Zhang, R. Hadfield, H. Robert, T. Honjo, K. Tamaki, and Y. Yamamoto, “Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors”, *Nature Photonics* **1**, 343--348 (2007).

7. B. B. Elliott, O. Pikalo, J. Schlafer, and G. Troxel, “Path-length control in an interferometric QKD link”, *Quantum Information and Computation, Proceedings of the SPIE* **5105**, 26--38 (2003).

8. V. Makarov, A. Brylevski, and D. R. Hjelme, “Real-time phase tracking in single-photon interferometers”, *Journal Applied Optics* **43**, 4385--4392 (2004).

9. M. Hendrych, PhD thesis *Experimental Quantum Cryptography*, Joint Laboratory of Optics of Palacky University and Institute of Physics of the Czech Academy of Sciences.

10. Q. Xu, M.B. Costa E Silva, J-L. Danger, P. Gallion and F. J. Mendieta, “Towards quantum key distribution system using homodyne detection with differential time-multiplexed reference”, *5th IEEE International Conference on Information and Communication Technologies RIVF 2007 Hanoi, Vietnam*, (March 2007).

11. C. W. Helstrom, *Quantum Detection and Estimation Theory, Mathematics in science and Engineering* **123**, (New York: Academic Press, 1976).

12. Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, “One way differential QPSK quantum key with channel impairment compensation”, *CLEO/Europe-IQEC*, JSI-3 (2007).

13. Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, “Auto-compensating quantum crypto-system using homodyne detection”. *Optical Fiber Communication Conference, OFC 2008*, JWA49 (San Diego, California, 2008).

14. Q. Xu, M. Sabban, P. Gallion and F.J. Mendieta, “Quantum key distribution system using dual-threshold homodyne detection”, *6th IEEE International Conference on Information and Communication Technologies RIVF 2008* Hanoi, Vietnam (2008).

CHAPTER 7 QPSK QUANTUM KEY DISTRIBUTION USING PHOTON COUNTING

Bennett first mentioned the phase encoding QKD system for the two-state protocol BB92 [1]. Provided that the coherence length of the light used is larger than the path mismatch, interference fringes can be recorded, thus the interferometers become a very natural choice to implement a fiber-optic system for the facility of transmission.

In this chapter we first review the principle of photon counters for QKD system, then we evaluate the interferometric system performances in free-running conditions. Finally we introduce a method to improve photon counting operationality with optical phase synchronization using training frames.

7.1 PHOTON COUNTING PRINCIPLES

As we have already mentioned in chapter 3.4, with the pseudo single photon source, the success of quantum crypto-system depends essentially on the ability to detect signal photons. The ideal photon detector should comply with the following requirements:

1) The quantum detection efficiency should be high over a large spectral range;

2) The probability of generating dark counts and after pulse counts should be small;

3) The time between the detection of a photon and generation of an electrical signal should be as constant as possible, i.e., the jitter should be small, so as to ensure good time resolution;

4) The quenching process after the gate operation should be short so as to allow high data rates.

The best figure of merit for quantum crypto-system is the ratio of dark-count rate R_{Dark} to the detection efficiency η, as defined noise equivalent power (NEP):

$$NEP = \frac{h\nu}{\eta}\sqrt{2R_{Dark}} \tag{7.1}$$

Here h is the Planck's constant and ν is the frequency of the impinging photons.

7.1.1 Photon Counting Silicon APD at Wavelength Below 1.1 μm

Much work has been done since 1980s to improve the silicon APD for single-photon counting [2-6], and the performance has accordingly been continuously improved. Si APDs have replaced the precedent photon-multiplier tubes. High quantum efficiency up to 76% [7] and very low time jitter of 28 ps [8] has been reported. Today the commercialized Si APD can have typical quantum efficiency around 70% at 700 nm and dark count rates of 50 counts/s under precise temperature control of 253 K, and jitter time as low as 300 ps (e.g., EG&G SPCM-AQ-151) at operation frequency 5 MHz.

These silicon APD single photon counters are ideal for quantum cryptography applications in free space and in optical fibers. However at these wavelengths the transmission loss is very high in the optical fiber, and the working distance is the bottleneck for the optic-fiber system.

7.1.2 Photon Counting InGaAs/InP at Telecom Wavelengths

In the second (1300 nm) window, germanium or InGaAs/InP semiconductor materials are the best choices, and in the third (1550 nm) window the only option is InGaAs/InP. However, the quantum efficiency is much lower at telecommunications wavelength. To date, no industrial effort has been successfully to optimize APD's operating at telecommunications wavelengths for photon counting, and their performance still lags far behind that one of silicon APD's. The physical reasons for the lack of high-performance commercial products are, first, the common semiconductor material is not sensitive enough to this wavelength; and second, the market for photon counting is not yet mature.

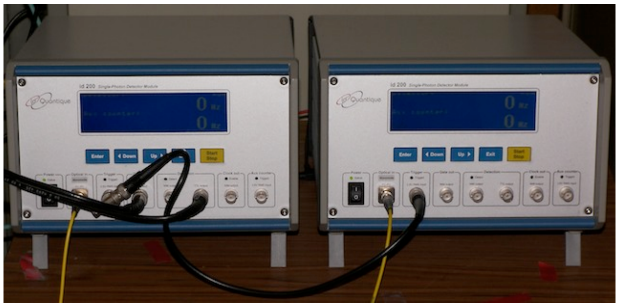


Figure 7.1 Id Quantique id200

In our experiments we use 2 Id Quantique id200 single photon detector modules (SPDM) [9] as shown in Figure 7.1. The instruments integrate the APD at telecommunications wavelength and the electronic parts, allowing flexible external/internal trigger input for “gating operation command”. When working at a stable temperature of 220 K, the quantum efficiency is around 10%, and the dark count rate increases with quantum efficiency when a larger gate width is selected.

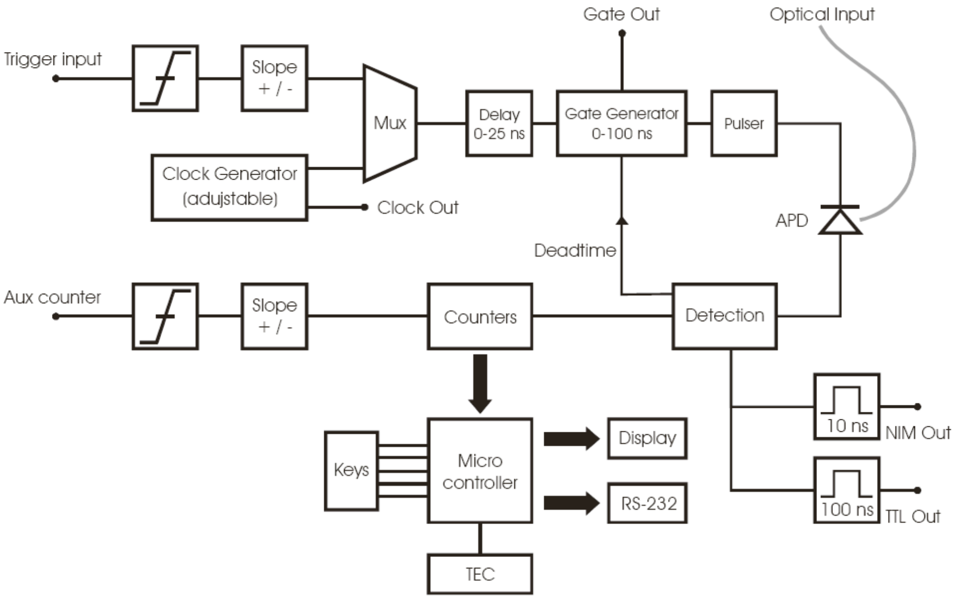


Figure 7.2 Block diagram of the id 200 SPDM

A variable dead time can be selected to suppress afterpulse occurrences. Dead time can be set to 0, 1μs, 2μs, 5μs, 10μs, so as to suppress the detrimental afterpulsing effects. A gate generator unit and a pulser unit produce a gate with the appropriate duration and amplitude. Five different values of the gate width can be generated: 2.5ns, 5ns, 20ns, 50ns or 100ns. Gate widths of 2.5ns and 5ns result in an effective gate of typically 500ps and 1.5ns for arriving photons. These short gates provide a very low noise level for applications where the arrival time of the photon is known with high accuracy.

The photon detection probability is around 10%, independent of gate width and trigger frequency. The maximum operational frequency is limited to 4 MHz due to the quenching process.

7.2 TIME-MULTIPLEXING INTERFEROMETER

Interferometric homodyne arrangements are usually used for the implementation of phase detection, in which the key issue is to obtain a phase reference at the receiver end. Using a separate fiber for reference transmission leads to difficult stabilization on an interferometer over the complete span of the transmission link, and a one-way and single path configuration is mandatory to avoid round trip penalty [10]. For that reason, Merolla has proposed [11] a self-phase referencing QKD system in the frequency domain that utilizes carrier and phase modulation of sidebands. A differential phase shift keying (DPSK) is also an effective way to provide phase reference by relaxing the phase stabilization over time duration of the same order of the bit period. DPSK demodulation by delay line has been extensively discussed during the early age of optical communications [12-14] and more recently [15,16].

7.2.1 DOUBLE MACH-ZEHNDER CONFIGURATION OF QPSK BB84 SYSTEM

Figure 7.3 is our experimental setup for the photon counting system [17] based on the QPSK self-homodyne setup. Now that Alice and Bob are spatially separated, the setup will suffer from poor performance owning to environmental perturbations. In order to stabilize the interference, the difference of the optical lengths of the interferometer's arms must be kept constant within a fraction of the lightwave wavelength. Therefore using a single interferometer for Alice and Bob as shown in Figure 6.1 cannot remove the impairments. Temperature fluctuations and mechanical vibration from the environment in a two-fiber path optical interferometer can result in different phase and polarization changes and smearing out interference as well. For that reason, both paths of the interferometer are combined and launched into a time shared single mode fiber; the time-multiplexing interferometer can thus eliminate a large part of the environmental fluctuations in the transmission common fiber, leaving the phase and polarization stabilization to small local interferometer that is independent of the transmission distance.

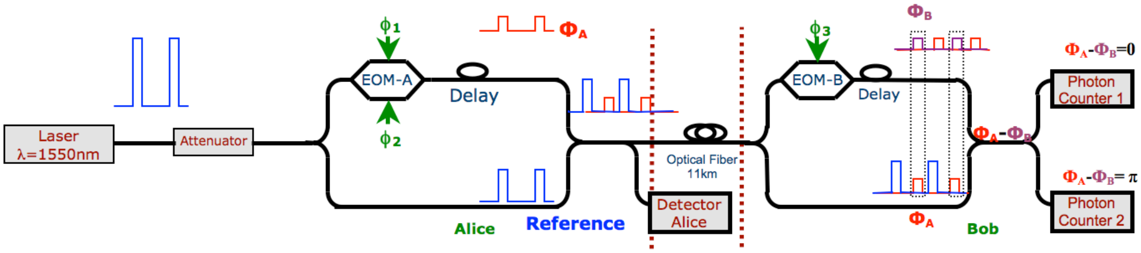


Figure 7.3 QKD QPSK Setup: Photon Counting Detection (dot lines correspond to the gate time)

As shown in Figure 7.3, the system is composed of two identical unbalanced interferometers. Thus no interference occurred in the small interferometers. Fiber couplers perform 50:50 splitting of lightwave beam, and the length differences at Alice's side and at Bob's side are equal to 3 meters of single mode fiber.

In such a system, the pulsed laser is attenuated to a quantum level before entering the system. Since EOM-A and EOM-B have the same insertion loss, we apply Alice's and Bob's phase modulations both in the longer arm of the two unbalanced interferometers so that the pulses of the signal and those of reference have the same intensity.

The coherent receivers require accurate phase synchronization, which imposes severe requirements on the receiver structure. In our first configuration, we send a signal pulse that carries information on its phase, together with a time-multiplexed reference, thus to simplify the detection and to relax the polarization and phase stability requirements to very short interval duration.

If we apply plane wave approach for the photon counting detection scheme (Annex B) using Detectors *D1* and *D2*, and assuming that $E_S = E_{LO}$ and $\Phi_A - \Phi_B = \theta$, we can have:

$$\begin{cases} D_1 = 2{E_S}^2(1+\cos\theta) \\ D_2 = 2{E_S}^2(1-\cos\theta) \end{cases} \tag{7.2}$$

The photon arrives on the output D_1 when $\theta = 0$ or arrives on the output D_2 when $\theta = \pi$. There is no intrinsic BER thanks for an ideal SPDM. However it is limited by the interferometer fringe visibility due to the residual polarization mismatch and also by the after-pulses induced by the precedent avalanche current.

7.2.2 Quantum Bit Error Rate

We assume the wrong bits number is N_{wrong} and right bits number is N_{right}, and the quantum bit error (QBER) is defined as the ratio of the wrong bits number to the total number of bits received and is normally on the order of a few percent. We can express it as a function of rates:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{error}}{R_{sift} + R_{error}} \tag{7.3}$$

Here R_{error} is the error key rates and $R_{sif\,t}$ is the sifted key rates.

Since the sifted key rate corresponds to the case in which Alice and Bob made the choices of bases, according to the protocol BB84, it is ideally 50% of the repetition rate. The raw key rates depend on, naturally, the pulse repetition rate f_{rep}, the mean photon number per pulse μ, the probability that the photons arriving on the detectors t_{link}, e.g. photons can be absorbed in the propagation channel, leading to attenuation, as well as the probability η that the arriving photon being detected i.e. quantum efficiency of the detector):

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} f_{rep} \mu t_{link} \eta \tag{7.4}$$

We can also indentify that there are three main facts that contribute to the error key rate R_{error}:

1) The rate that photons arrive on the wrong detectors R_{opt} due to the imperfect interference or the polarization contrast;

2) The dark counts rate R_{dark} of the photon detectors that is independent of the bit rate, but is related to the gate width and the "dead-time" in that a longer time window give rise to more dark counts errors;

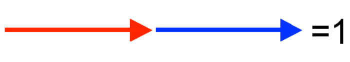
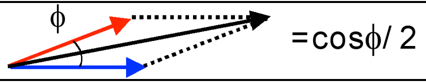
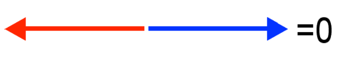
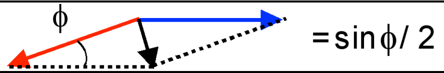
3) The additional system impairments R_{acc}

We can thus have $R_{error} = R_{opt} + R_{dark} + R_{acc}$, also

$$\begin{aligned} QBER &= \frac{R_{opt} + R_{dark} + R_{acc}}{R_{error} + R_{sift}} \\ &= \frac{R_{opt}}{R_{error} + R_{sift}} + \frac{R_{dark}}{R_{error} + R_{sift}} + \frac{R_{acc}}{R_{error} + R_{sift}} \\ &= QBER_{opt} + QBER_{dark} + QBER_{acc} \end{aligned} \tag{7.5}$$

In most experimental quantum crypto-system, the first term is the dominant effect that measures the optical quality of the setup since it depends only on the polarization and the interference fringe contrast. In a fiber-optic system, it is essential to obtain and maintain a constant low $QBER_{opt}$ in spite of the polarization fluctuations and depolarization in the fiber link. If the signal and reference pulses have a phase mismatch ϕ, the interference visibility V will change accordingly.

Table 7-1 Quantum bit error rate (When “1” is transmitted)

	Ideal interferometer	Non-ideal interferometer
D1		
D2		
	Fringe Visibility: $V=1$	Fringe Visibility: $V=\cos\phi$

As we show in Table 7.1, the QBER of photon counting is issued mainly from the phase fluctuation, and this condition is valid only when $L = S$. The received $QBit$ is:

$$|QBit\rangle = \cos(\phi/2)|1\rangle + \sin(\phi/2)|0\rangle \qquad (7.6)$$

As the received signal is no more on eigen state,

$$p(1/0) = p(0/1) = \sin^2(\phi/2) \qquad (7.7)$$

For a phase-encoding system, the $QBER_{opt}$ is directly related to the interference visibility V in that:

$$QBER_{OPT} = p(0)p(1/0) + p(1)p(0/1) = \sin^2(\phi/2) = \frac{1-V}{2} \qquad (7.8)$$

Good visibility implies very well aligned and stable interferometers. In single-mode fiber perfect mode overlap between signal and reference can be achieved automatically and polarization must be well controlled. Using polarization-maintain components in interferometers can be a good solution, by considering chromatic dispersion as a negligible problem for the detection part.

The second term $QBER_{Dark}$ increases with the propagation distance since the dark-count rate is constant while the raw bit rate decreases with t_{link} and fewer photons can arrive at the receiver's end. It is the detector noise that limits the transmission distance. For example, id 200 SPDM has announced dark count probability at gate width 2.5 ns as $P_{dc} < 5 \times 10^{-5}$, when working at repetition frequency $f_{rep} = 4MHz$, the dark-count rate per second is thus: $P_{dc} f_{rep} < 5 \times 10^{-5} \times 4 \times 10^{6} = 200$ counts/second. In our experiments, we obtained around 180-190 dark counts per second.

The third term $QBER_{acc}$ is present when multi-photon pulses are processed in such a way that they do not necessarily encode the same bit value. In phase encoding system this error can happen when only the signal pulse or the reference pulse arrives on the combiner (optical coupler) and the other is lost, either in the propagation fiber that links the sender and the receiver or in the interferometers. Unequal signal pulse and reference pulse levels can also induce such errors.

7.3 EXPERIMENTAL IMPLEMENTATION USING PHOTON COUNTING

We have implemented an experimental one-way and one-path QKD system with QPSK modulation. Figure 7.4 and 7.5 present our experimental setup.

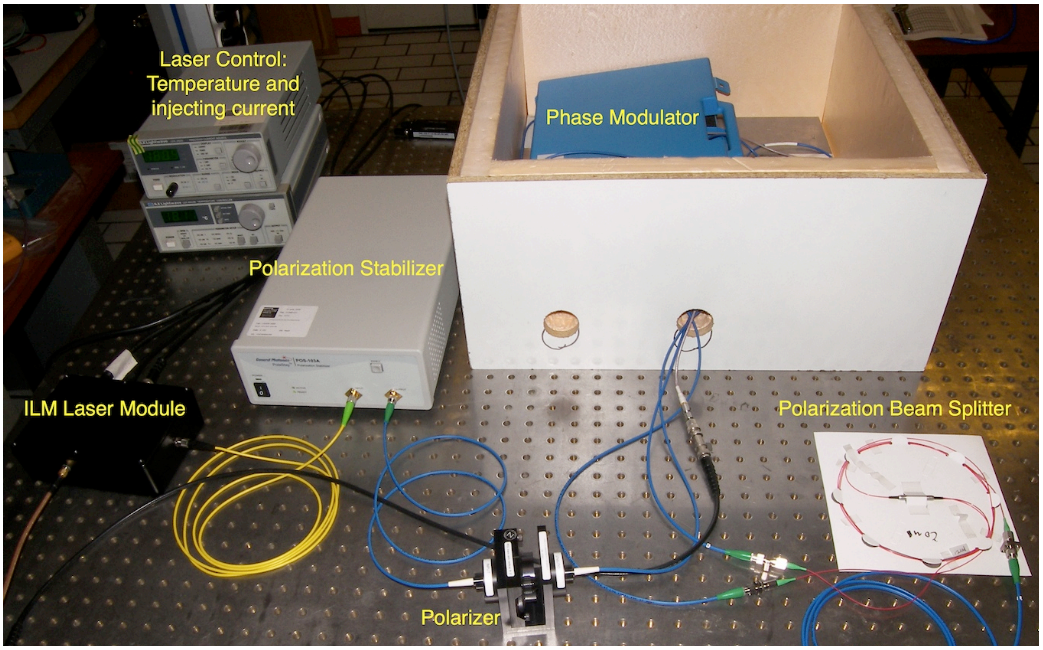


Figure 7.4 Alice’s experimental setup

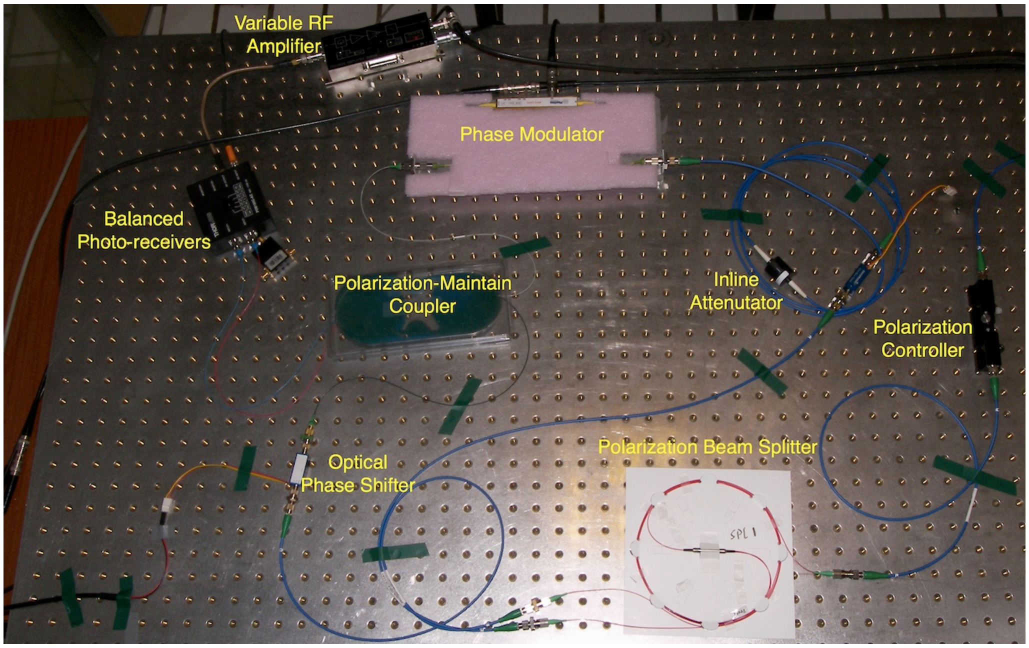


Figure 7.5 Bob’s experimental setup

7.3.1 PHOTON COUNTING UNDER FREE-RUN CONDITION

In our first experiment the repetition frequency was set to 4 MHz and the gate width was set to 2.5 ns so as to minimize the dark count rate. We have tested the quality of the interferometer under free-run condition.

We have measured the number of received photons by each detector (Detector 1 and Detector 2) during an interval of every 0.2 second. Figure 7.6 shows a measurement of the sum of received photon numbers by Detector 1 and Detector 2 over more than 5 hours. Meanwhile, the slow polarization change degrades since the modulators are both polarization-sensitive. The arriving photons can go to either of the detectors but the sum of the counts remains almost constant except some short term fluctuations.

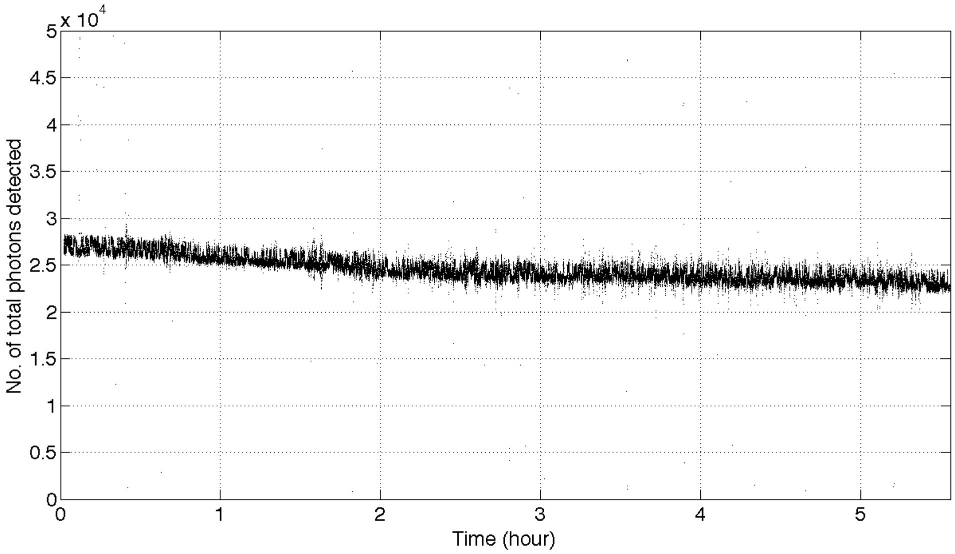


Figure 7.6 Number of photons detected by two detectors under free-run condition

This is also one method to measure the mean signal power since it is impossible to measure the optical power of the quantum level signal using optical power-meter. In the above experiment, the repetition frequency is $f_{req} = 4MHz$ and the sum is around 2.5×10^4 photons per 0.2 second, corresponding to 1.25×10^5 photons per second. Since the optical power is very weak, we consider the probability that multi-photons arriving on both detectors during the same time slot (gate operation) negligible. The detectors have received 1.25×10^5 photons during 4×10^6 "gate" operations, i.e., 3.12% of the bits have been received by one of the two detectors. As the quantum efficiency is around 0.1, and the reference pulse and the pulse have the same mean intensity, therefore the average impinging signal pulse has about 0.15 photon/bit.

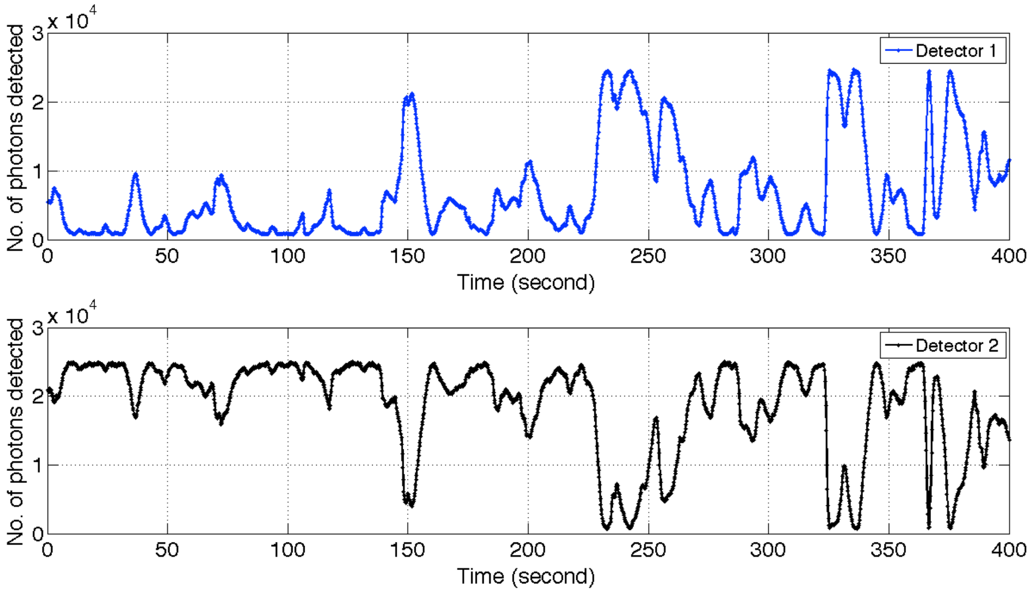


Figure 7.7 Free-run photon counts of the two detectors, the number of detected photon is measured every 0.2 second from each detector.

The two detectors have slightly different intrinsic quantum efficiencies that also change over time due to the optical beam polarization variation and their internal circuit. As well the minimum count and the maximum count per 0.2 second are 800 and 26000, respectively; thus the finest achievable $QBER$ is around 2% - 3%. As we have mentioned before the dominant term is $QBER_{opt}$ that is issued from the imperfect interference fringe contrast, the imperfect polarization extinction ratio of the reference pulses, and the polarization mismatch between the signal pulse and the reference pulse. The second contribution $QBER_{dark}$ is measured to be around 36-40 counts per 0.2 second. The third term $QBER_{acc}$ due to the unequal signal and reference wave intensity mixing appears to be much smaller than the other two terms.

7.3.2 Photon Counting for QPSK Modulation

At Alice's end we modulate on the upper arm (Figure 7.3) of the Mach-Zehnder interferometer to generate signal pulses which carry phases (Φ_A: $\pi/4$ and -3 $\pi/4$ in base A1; - $\pi/4$ and 3 $\pi/4$ in base A2); and at Bob's end on the upper arm we modulate the reference pulses originating from Alice's interferometer's lower arm, thus generating reference pulses that carry (Φ_B: $\pi/4$ in Base B1, - $\pi/4$ in Base B2) [18]. This setup has been designed also to help compensate for the insertion loss of the electro-optic modulator (EOM), which is around 4 dB. In other words, if we modulate at Bob's end the signal pulse that carries Φ_A, to generate a $\Phi_A - \Phi_B$ phase pulse before beating with the non-modulated reference pulse, we would lose additional 4 dB in the weak signal pulses.

The histogram in Figure 7.8 shows the situation for the coincidence of Alice and Bob's base choice. The histogram in Figure 7.9 shows the situation for the anti-coincidence case. We have fixed the phase shift on both Alice's and Bob's modulators, so as to evaluate the system performance. In the case of base coincidence when $\Phi_A - \Phi_B = \pi$ or 0, ideally no photon arrives at counter 1(2) (the first histogram of Figure 7.8) and all photons would arrive at the counter 2(1) (the second histogram of Figure 7.8). In the case of base anti-coincidence where $\Phi_A - \Phi_B = \pm\frac{\pi}{2}$, all the arriving photons click randomly on counter 1 or counter 2, as shown in Figure 7.9.

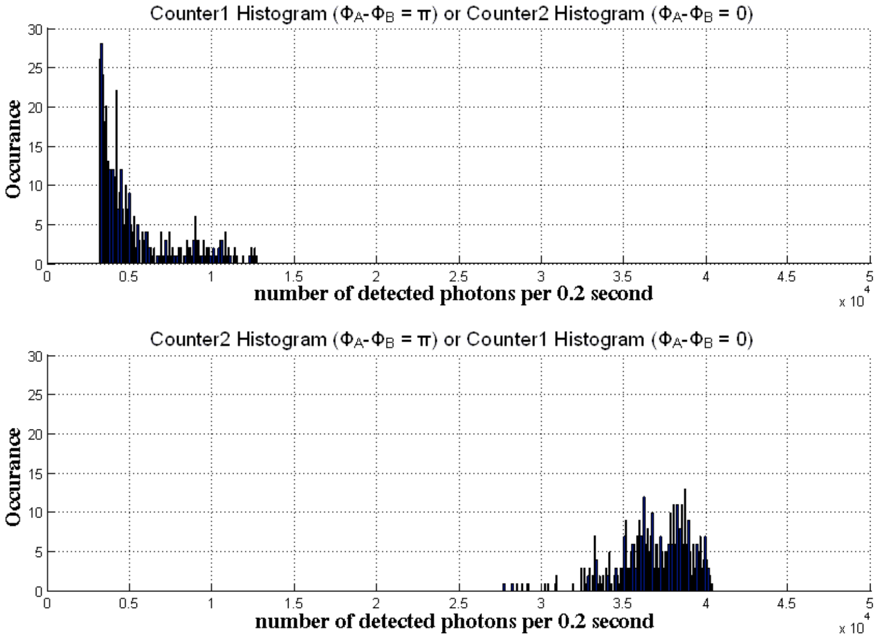


Figure 7.8 Histogram of Base Coincidence (when Alice and Bob choose the same base for a certain bit, $\Phi_A - \Phi_B = \pi$ or 0)

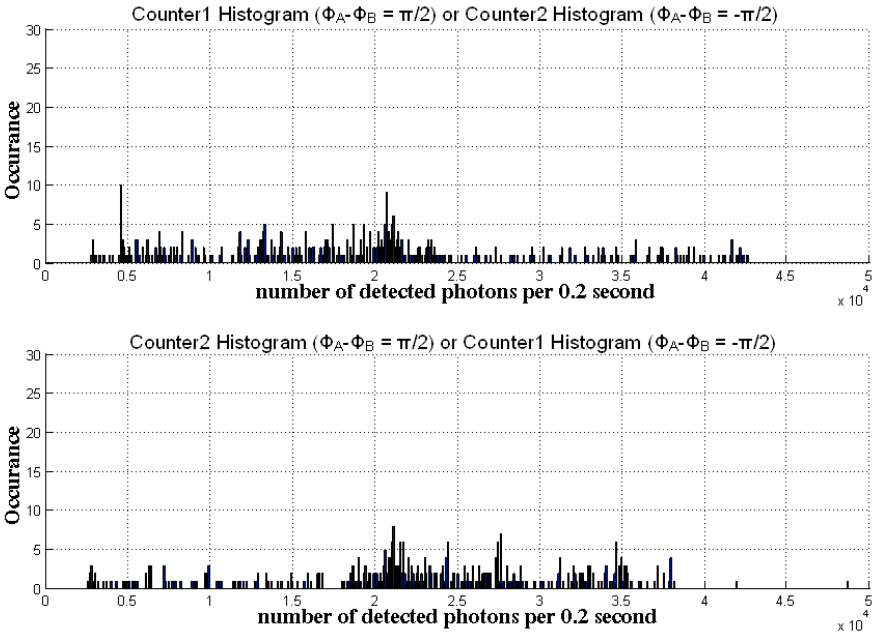


Figure 7.9 Histogram of Base Anti-Coincidence (when Alice and Bob choose different bases for a certain bit, $\Phi_A - \Phi_B = \pm\pi/2$)

Even though a finest visibility of 97%-98% is obtainable, the phase drift issues caused by the unavoidable thermo-mechanical variations must be handled for a practical system, as we have introduced in chapter 6 using phase compensation feedback loop and polarization splitting scheme is mandatory. Our main works focus on decreasing the R_{opt} contribution by improving the interference fringe contrast and polarization match, as well as constructing a feedback to compensate for the phase drift.

7.3.3 Improved Photon Counting QPSK Quantum Crypto-system

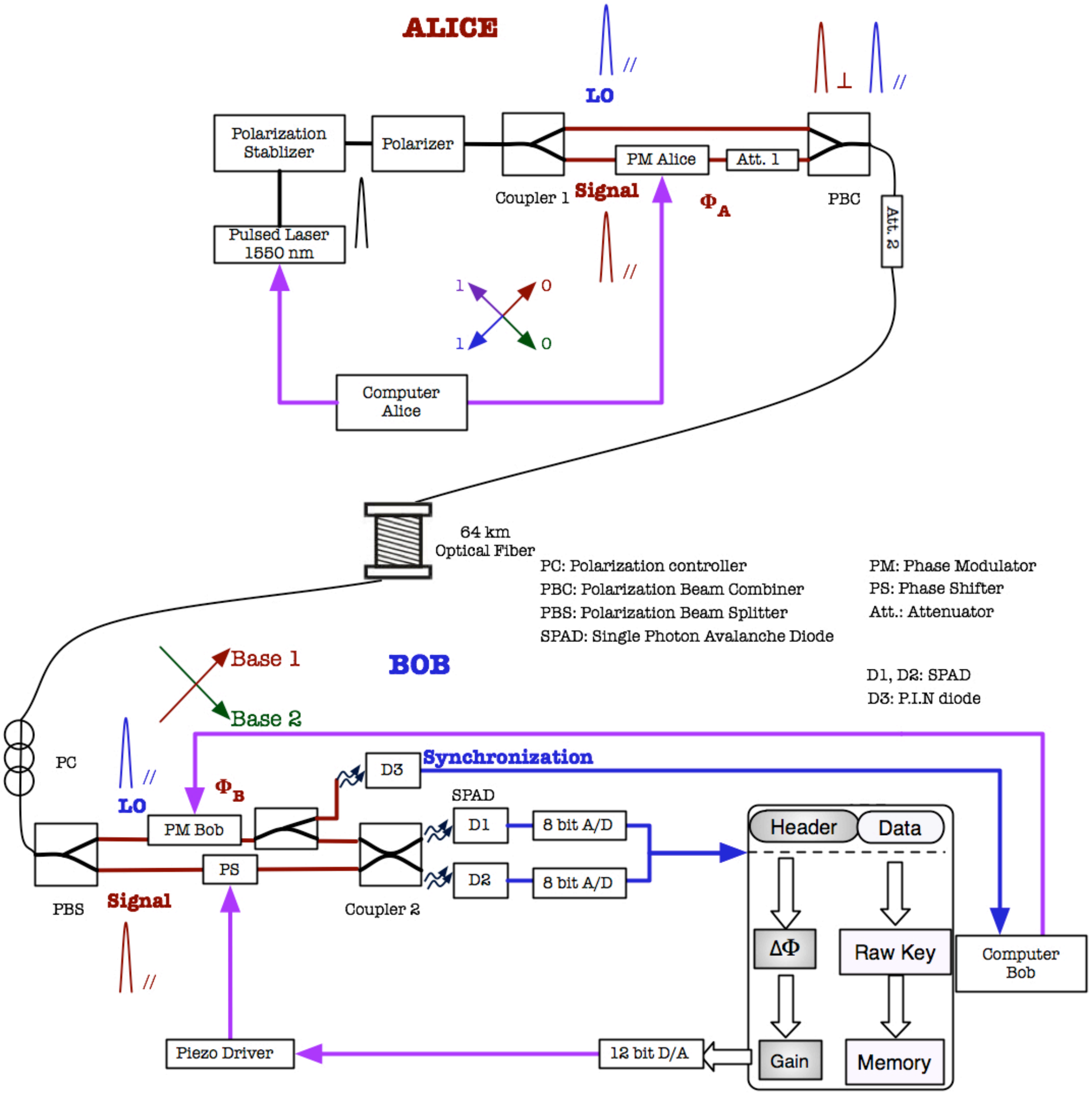


Figure 7.10 Improved experimental setup for photon counting QKD system

As shown in Figure 7.10, we have improved the experimental QKD system based on the same protocol as the setup shown in Figure 7.3. We use a 1550 nm ILM laser source to generate pulses of 5 ns width with 18 dB intensity extinction ratio, and the operational frequency is also limited to 4 MHz.

We use a General Photonics polarization stabilizer to actively maintain a stable output state of polarization (SOP) and to eliminate polarization fading. A polarization splitting method [19, 20] is used in our setup to improve the isolation of the signal and the strong reference field, since the 18 dB intensity extinction ratio alone is not enough for the time-multiplexing of the weak signal and the strong LO field. Alice's laser pulses are separated by a 50/50 polarization-maintain coupler, and propagate through the upper and lower arms of a Mach-Zehnder interferometer constructed with polarization maintaining (PM) fibers.

Alice encodes her lower arm pulses (Φ_A: π/4 and -3π/4 in base A1; -π/4 and 3π/4 in base A2) on a Lithium Niobate phase modulator (Photline MPX), constituting a QPSK modulation. The weaker signal and the un-modulated LO pulses are time-multiplexed by a polarization-beam-combiner (PBC), and the delay between the two components is set to be 20 ns, i.e. the inline attenuator and the phase modulator consist of 2 meters of optical fiber, respectively. Orthogonally polarized, the signal pulses and the LO pulses propagate with a high degree of isolation. Attenuator 1 is used to generate the weak coherent states (WCS) signal pulses and attenuator 2 is used in the photon-counting scheme to match the signal and LO powers.

Then the combined signal-LO pulses pass through a QKD link in a standard telecom single mode fiber (SMF). Bob uses a polarization-beam-splitter (PBS) with a polarization extinction ratio of 25 dB to separate the horizontally polarized LO pulses and the vertically polarized signal pulses. A small portion of the LO component is picked up for the receiver synchronization, using a PIN diode D3.

Bob's receiver has a similar Mach-Zehnder interferometer structure. He performs the LO phase shift in the upper arm on a Lithium Niobate phase modulator to apply his base choice (Φ_B: π/4 in Base B1, -π/4 in Base B2), constituting a BPSK conversion in which $\Phi = \Phi_A - \Phi_B$. The delay between the signal and the LO pulses is carefully adjusted to 20 ns to optimize the time overlap on the PM coupler's input ports with the same state of polarization (SOP).

To keep the system unconditionally secured, the QBER threshold must remain under 11% with a reduced key generation rate, and the corresponding phase error is $\Delta\Phi \approx 27°$ [20]. In our setup, the phase drift $\Delta\Phi$ is compensated by an optoelectronic feedback using a phase shifter (PS) in Bob's lower arm. A periodical interval of *M* bits is used as "training frame header" so as to compute the phase drift in the system in order to feedback on the PS. The training frames contain predetermined sequences on which Alice and Bob agree on the symbols and bases. The piezo-driver fiber actuator allows a dynamic range [-8π, 8π] and a response time of few milliseconds.

The mean value of *M* bits in the "training frame header" is close to the normal distribution $\mathrm{N}\left(\mu,\sigma/\sqrt{M}\right)$, in which μ is the expected value and σ is the standard deviation of an individual sample. As mentioned in chapter 6.5.2 when an uncertainty in amplitude estimation less than error *E* (relative to μ) is required, the following condition must be met:

$$erfc\left(\sqrt{2M}/2\sigma\right) \approx \exp\left(-M/2\sigma^2\right) < E \tag{7.9}$$

For example, assuming the unity is the amplitude of one photon, then the standard variation $\sigma = 1/2$. If the mean signal pulse power is $\mu = 0.01$, then the standard deviation is $\sigma' = \sigma/\mu = 50$; and we expect a good precision of measurement as 99.99%, hence $E = 1 - 99.99\% = 10^{-4}$. Consequently we can obtain:

$$\begin{aligned} &\exp\left(-M/2\sigma'^2\right) = \exp\left(-M/5000\right) < E = 10^{-4} \\ &\Rightarrow M > 46052 \end{aligned} \tag{7.10}$$

We use two single photon detection modules (SPDM, id 200, id Quantique) as D1 and D2 (Single Photon Avalanche Diode: SPAD) in Figure 7.10. The output of the SPDM is a pulse TTL of 100 ns width when a detection event occurs. We have implemented an 8-bit analog/digital converter (ADC) for the pulse detection and the recording of the photon arrival time.

For a short gate operation of 2.5 ns, we consider that the dark count probability for *D1* and *D2* are ε_1 and ε_2, respectively; the quantum efficiencies are ρ_1 and ρ_2 (ρ_1, $\rho_2 < 0.1$); and the interferometer visibility is V. Then, during this gating operation, the probabilities that *D1* or *D2* records a detection event are:

$$\begin{cases} P_{D1}(\Phi) = \varepsilon_1 + \rho_1 \dfrac{1 + V\cos\Phi}{2} \\ P_{D2}(\Phi) = \varepsilon_2 + \rho_2 \dfrac{1 - V\cos\Phi}{2} \end{cases} \tag{7.11}$$

In the course of the "training frame header" interval, we use eight registers to record the incoming events, i.e., {$R_{D1,0}$, $R_{D1,\pi/2}$, $R_{D1,\pi}$, $R_{D1,3\pi/2}$} for *D1* and {$R_{D2,0}$, $R_{D2,\pi/2}$, $R_{D2,\pi}$, $R_{D2,3\pi/2}$} for *D2* to store the number of detection events for $\Phi = 0, \pi/2, \pi, 3\pi/2$.

For D1,

$$\begin{cases} P_{D1}\left(\dfrac{3\pi}{2}\right) - P_{D1}\left(\dfrac{\pi}{2}\right) = \rho_1 V \sin\Delta\Phi \\ P_{D1}(0) - P_{D1}(\pi) = \rho_1 V \cos\Delta\Phi \end{cases} \tag{7.12}$$

For D2,

$$\begin{cases} P_{D2}\left(\dfrac{3\pi}{2}\right) - P_{D2}\left(\dfrac{\pi}{2}\right) = -\rho_2 V \sin\Delta\Phi \\ P_{D2}(0) - P_{D2}(\pi) = -\rho_2 V \cos\Delta\Phi \end{cases} \tag{7.13}$$

From (7.12) and (7.13), we can easily obtain an approximate value of the real-time phase error $\Delta\Phi$. A 12-bit digital/analog converter (DAC) outputs the voltage to be applied on the phase-shifter to compensate the phase error every 0.1 second. Figure 7.11 shows our experimental results for a measured phase error and the residual QBER when the signal mean photon number per bit N_S is 0.5 (the probability of detecting an arriving photon is 0.05 since the quantum efficiency is 0.1).

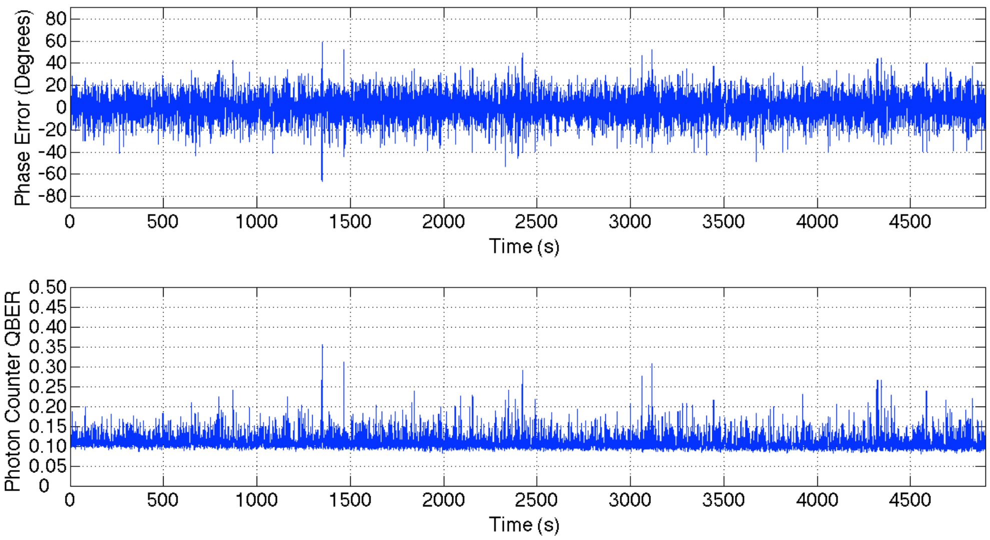


Figure 7.11 Photon counting system residual phase error and its QBER

We have taken 10% of the all data for the training frame so as to guarantee a precise phase tracking, and we managed to stabilize the system phase over a long tern operation. The residual phase error appears as a simple attenuation of the incoming signal, leading to a higher error rate for a given signal photon number. It is also due to the DAC quantification error, the piezo-driver precision jitter, and the phase-shifter delay as we correct the phase error only every 0.1 later instead of real-time.

We will discuss the system performance in terms of detection efficiency, and BER and the security issues more in detail in the next chapter as for the comparison with the balanced homodyne detection scheme.

REFERENCES

1. C. H. Bennett, “Quantum cryptography using any two nonorthoganol states”, *Physical Review Letters* **68**, 3121--3124 (1992).

2. T. E. Ingerson, R. J. Kearney, and R. L. Coulter, “Photoncounting with photodiodes”, *Applied Optics* **22**, 2013--2018 (1983).

3. R. G. W. Brown, K. D. Ridley, and J. G. Rarity, ‘‘Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching,’’ *Applied Optics* **25**, 4122--4126 (1986).

4. R. G. W. Brown, R. Jones, J. G. Rarity, and K. D. Ridley, ‘‘Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching’’, *Applied Optics* **26**, 2383–2389 (1987).

5. R. G. W. Brown, and M. Daniels, “Characterization of silicon avalanche photodiodes for photon correlation measurements. 3: Sub-Geiger operation”, *Applied Optics* 28, 4616--4621 (1989).

6. A. Spinelli, L. M. Davis, and H. Dauted, “Actively quenched single-photon avalanche diode for high repetition rate time-gated photon counting”, *Review of Scientific Instruments* **67**, 55--61 (1996).

7. P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff, “High-efficiency single-photon detectors”, *Physical Review A* **48**, 867--870 (1993).

8. S. Cova, A. Lacaita, M. Ghioni, and G. Ripamonti, ‘‘High-accuracy picosecond characterization of gain-switched laser diodes”, *Optics Letters* **14**, 1341--1343 (1989).

9. Id Quantique, “Single-photon detection with InGaAs/InP avalanche photodetectors”, *Single-Photon detector Module: Application note,* http://www.idquantique.com.

10. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “'Plug and play' systems for quantum cryptography”, *Applied Physics Letters* **70,** 793--795 (1997).

11. J.-M. Merolla, Y. Mazurenko, J. P. Goedgebuer, H. Porte, and W. T. Rhodes, “Phase-modulation transmission system for quantum cryptography”, *Optics Letters* **24**, 104--106 (1999).

12. T. Okoshi, “Recent advances in coherent optical fiber communication systems”, *Journal of Lightwave Technology* **5**, 44--52 (1987).

13. L. G. Kazovsky, “Balanced phase-locked loops for optical homodyne receivers”, *IEEE/OSA Journal of Lightwave Technology* **4**, 182--95 (1986).

14. T. Chikama, T. Naito, S. Watanabe, T. Kiyonaga, M. Suyama, and H. Kuwahara, “Optical heterodyne image-rejection receiver for high-density optical frequency division multiplexing system”, *IEEE Journal on Selected Areas in Communications* **8**, 1087--1094 (1990).

15. C. Xu, X. Liu, and X. Wei, “Differential phase-shift keying for high spectral efficiency optical transmissions”, *IEEE Journal of Selected Topics Quantum Electronics* **10**, 281--293 (2004).

16. A. H. Gnauck, and P. J. Winzer, “Optical phase-shift-keyed transmission”, *Journal of Lightwave Technology* **23**, 115--130 (2005).

17. M.B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, F. J. Mendieta, “Homodyne detection for quantum key distribution: an alternative to photon counting in BB84 protocol”, *Photonics North 2006, Proceeding of SPIE* **6343**, (2006).

18. Q. Xu, M. B. Costa E Silva, J.-L. Danger, S. Guilley, P. Bellot, P. Gallion and F. J. Mendieta, “Towards quantum key distribution system using homodyne detection with

differential time-multiplexed reference", *5th IEEE International Conference on Information and Communication Technologies RIVF 2007 Hanoi, Vietnam*, (2007).

19. Q. Xu, M. Sabban, M. B. Costa e Silva, P. Gallion and F. J. Mendieta, "Dual-threshold balanced homodyne detection in 1550nm optical fiber quantum cryptography system", To be published in *IEEE/OSA Journal of Lightwave Technology* (2009).
20. Q. Xu, M. Sabban, P. Gallion and F. J. Mendieta, "Quantum key distribution system using dual-threshold homodyne detection", *6th IEEE International Conference on Information and Communication Technologies RIVF 2008, Ho Chi Minh City , Vietnam*, (2008).

CHAPTER 8 QPSK QUANTUM KEY DISTRIBUTION USING DUAL-THRESHOLD BALANCED HOMODYNE DETECTION

We have discussed in the chapter 7 the implementation of a one-way experimental QKD system. In the optical telecom band, photon counters using avalanche diodes that work in Geiger mode under low and precise temperature control, exhibit inherent low quantum efficiency, high dark count rate, and inevitable residual after-pulse phenomenon due to the macroscopic avalanche process.

The key issue in a QKD system is the detection of quantum level signal, such as the reliable and inexpensive weak coherent states (WCP). Balanced homodyne detection (BHD), is sensitive to phase and polarization matching. Using high efficiency, high bandwidth and low cost positive-intrinsic-negative diode (PIN) operating at room temperature, facilitated by a strong local oscillator (LO), BHD scheme can constitute an interesting alternative to photon counting. In BHD only one quadrature is measured and there is no additional noise to the contribution of the zero-point fluctuation of the signal field. As reported by Yuen [1] the input signal quantum noise is, in this case, the only noise limitation and the LO noise has a negligible influence. Moreover, BHD has a frequency selection scheme that is useful for background radiation rejection as for the compatibility with the current WDM networks, and it can also use a LO of suitable power that provides noise free high mixing gain to overcome the thermal noise [2].

Furthermore the conventional PIN photodiodes operating at room temperature present much higher quantum efficiency and faster response speed as compared to the photon counters [3], also their cost is much lower and the supply requirements are much simpler. Operating near the quantum limit, it is free of the non-desirable effects such as afterpulses and “dark counts” characteristics of the single photon detection measurement (SPDM).

However, post-detection, threshold and symbol synchronization stages must be properly designed and based on received signal coincidence as in BHD as the decision process is carried out *a posteriori* [4,5], in opposite to photon counting for which the decision is a trade off between quantum efficiency and dark count [6,7].

In this chapter we first review the basics of BHD, before we introduce our QKD receiver structure. Next we present a one-way QPSK QKD system using dual-threshold BHD receiver with optical phase synchronization. Then we compare the performance of the QKD receivers using photon counting and BHD in terms of detection efficiency and BER (or QBER).

The optical phase and information recoveries are to be solved both by the receiver Bob and the eavesdropper Eve. Provided that the guarantee of security lies either on the mutual information gain or on the perception of eavesdropper's intervention, we will analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack, as well as the power modifying mixed attacks.

8.1 BALANCED HOMODYNE DETECTION FOR QKD SYSTEM

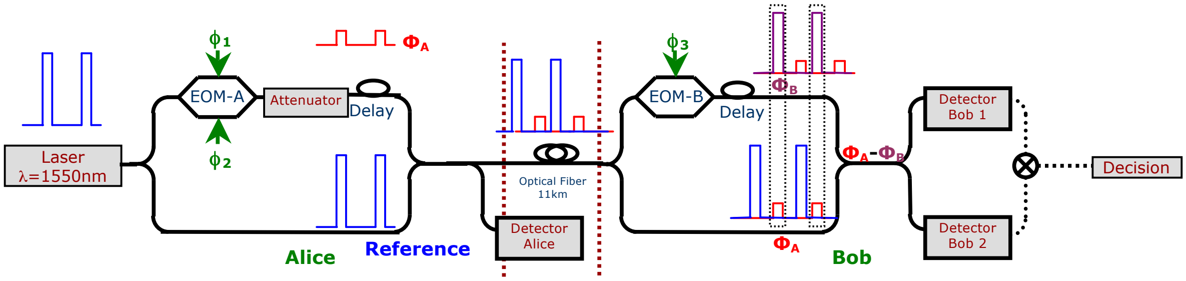


Figure 8.1 Preliminary QKD setup using balanced homodyne detection (dot lines are the observation window for the detected symbols)

BHD consists of mixing the weak signal filed with the strong LO field before intensity detection, i.e. $|E_{LO}| >> |E_S|$. If we apply the plane wave approach for the super homodyne detection scheme (Annex II) using Detectors *D1* and *D2*, we can have:

$$I_{balanced} = \left\| E_{signal} + E_{LO} \right\| - \left\| E_{signal} - E_{LO} \right\| = 4 E_S E_L \cos(\Phi_A - \Phi_B) \tag{8.1}$$

As we show in Figure 8.1, the modulated signal arm was constructed to have EOM-A followed by an optical attenuator, and Bob introduces his base choices in the reference arm at the reception. The configuration is similar to the photon counting detection scheme as we have shown in Figure 7.3, the main differences are in the detection part and the post-detection processing.

The balanced photo-receiver consists of two matched InGaAs photodiodes and a low-noise amplifier that generates an output voltage corresponding to the photocurrent difference between the two photodiodes, with a transimpedance gain of 40 V/mA. Figure 8.2 shows an example of the combination of the weak modulated signal pulses and the strong reference pulses at Alice's end. The weak modulated signal pulses are delayed as to constitute a time-multiplexing configuration.

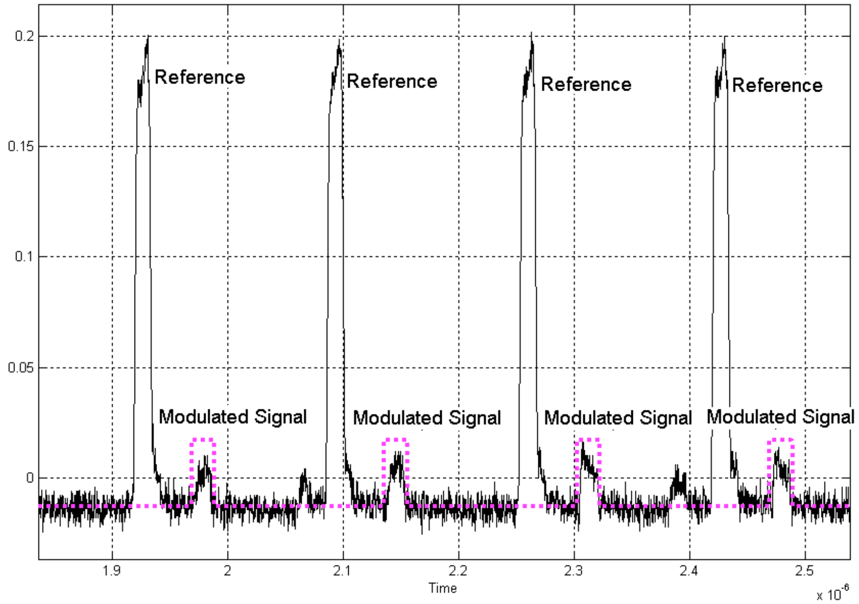


Figure 8.2 Alice's Output

The bits corresponding to the base coincidence (BC) have positive or negative levels, while those bits of base anti-coincidence (AC) are discarded (average level "zero"). In

Figure 8.3 we demonstrate Bob's detected symbols: the positive pulses stand for bits "1" (Φ_A - Φ_B = *0*) while negative ones stand for bits "0" (Φ_A - Φ_B = π), and AC cannot be discriminated (Φ_A - Φ_B = $\pi/2$ or $-\pi/2$).

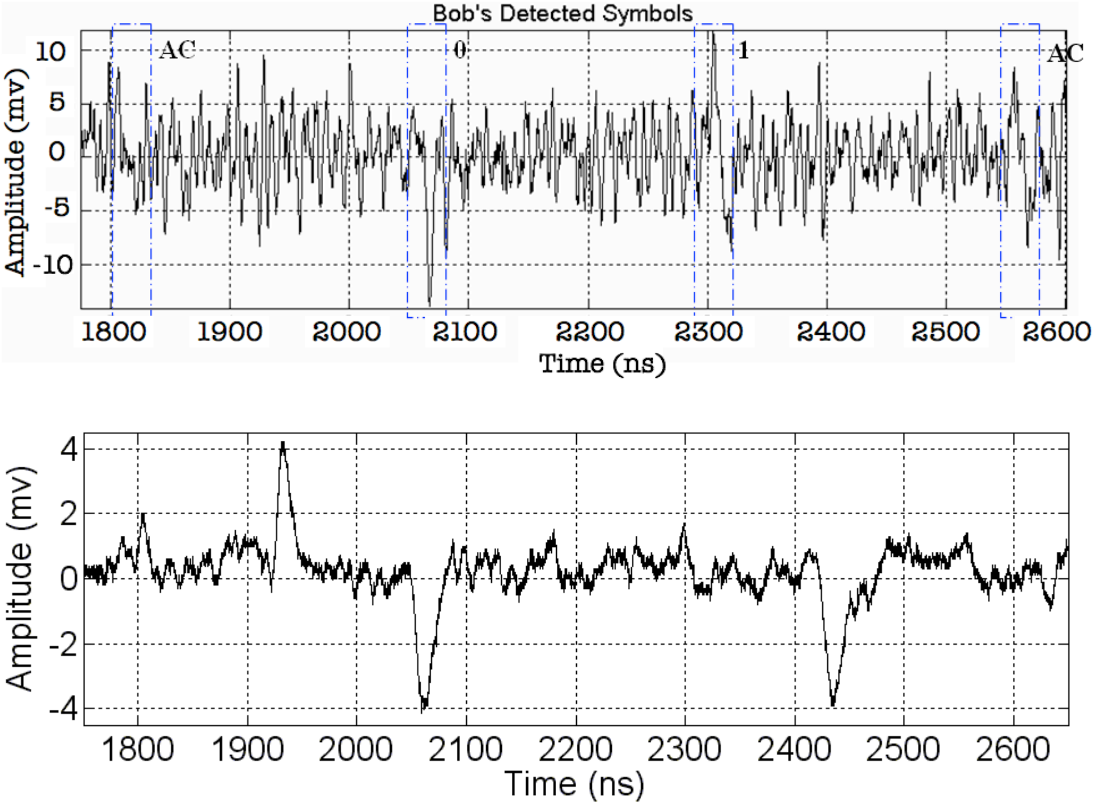


Figure 8.3 (a) Detection of Qubits without polarization splitting; (b) Detection of Qubits with polarization splitting scheme.

Compared to photon counting detection scheme, BHD improves the output signal-to-noise ratio (SNR) when a suitable reference power is employed. The "shot noise" is thus dominant since the strong reference pulse makes the thermal noise negletable ($noise_{thermal}$ = *-174dBm/Hz*, $noise_{shot}$ = *-152dBm/Hz* as measured in our experiments).

Furthermore BHD receiver is also very sensitive to polarization mismatching (Annex II), as we can see in the Figure 8.3 (a) and (b). In both two configurations using standard single mode fiber or using polarization-maintain components, the signal pulse power is around 2 photons/bit on average, however the noise level can be alleviated using polarization-maintain components, as we have mentioned in chapter 7. The output levels of the two measurements are slightly different because the reference pulses are not of the exact same power due to the polarization mismatch.

8.2 IMPROVED BHD QPSK QUANTUM CRYPTO-STYSTEM

8.2.1 SYSTEM SETUP

We have implemented the experimental one-way QPSK QKD system for the photon counting scheme and the BHD scheme as well, as mentioned in chapter 7.3.3. A flexible arrangement has been designed so that only slight changes have to be done to change the detection scheme from photon counting to BHD [8].

As shown in Figure 8.4, we use a 1550 nm ILM electro-absorption modulated light source to generate laser pulses of 5 ns width with 18 dB intensity extinction ratio. We also use a General Photonics polarization stabilizer followed by a polarizer to actively maintain a stable output state of polarization (SOP) and to eliminate polarization fading. For the sake of comparison with the photon counting detection scheme, the operational frequency is reduced down to 4 MHz. (In the BHD scheme, much higher repetition rates are attainable, however we chose to use 4 MHz as well for the ease of comparison.) Our balanced amplified photo-detector has a flat response passband from DC to 150 MHz (Thorlabs InGaAs switchable gain PDB150C-EC).

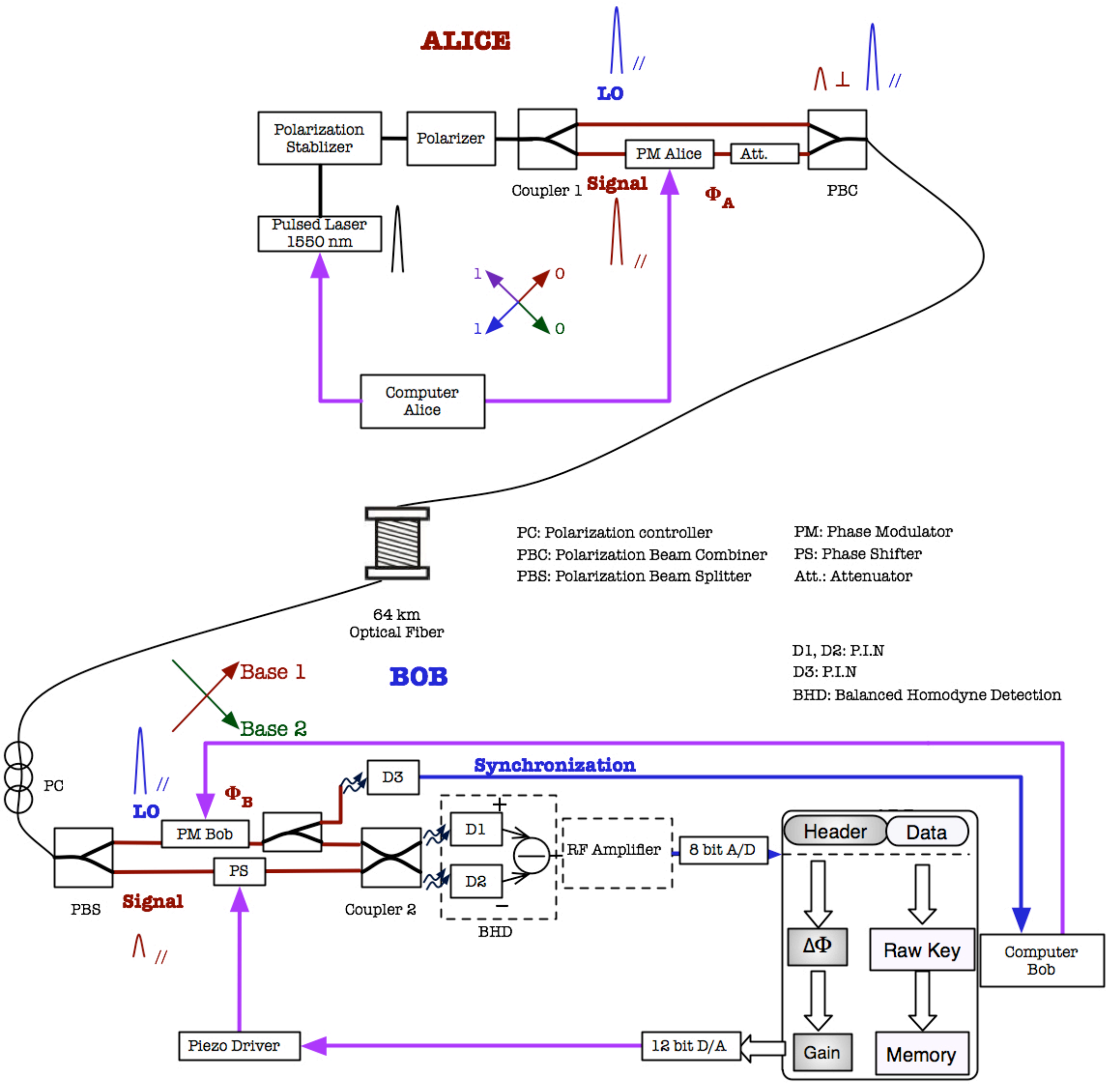


Figure 8.4 Experimental setup of QKD system using BHD

A polarization splitting method is also used in our arrangement so as to improve the isolation of the signal and the strong LO field. The polarization stablizer allows us to increase the injecting current at 180 mA to generate very strong laser pulses and meanwhile maintain the input polarization fluctuation less than 0.1 dB. Alice's laser pulses are separated by a 50/50 polarization-maintainng coupler, and propagate through the upper and lower arms of a Mach-Zehnder interferometer constructed with polarization maintaining (PM) fiber. No additional polarization control is required at Alice's end since the setup can constantly maintain the optimal SOP.

Alice encodes her vertically polarized pulses with phase modulation QPSK (Φ_A: π/4 and -3π/4 in base A_1; -π/4 and 3π/4 in base A_2) on a Lithium Niobate phase modulator (Photline MPX), constituting a QPSK modulation. The weak signal and the un-modulated LO pulses are recombined and time-multiplexed by a polarization-beam-combiner (PBC), and the delay between the two components is set to be 20 ns, i.e. 4 meters optical fiber. Orthogonally polarized with a polarization extinction ratio of 25 dB and an intensity distinction ratio of 18 dB, the signal pulses and the strong LO pulses propagate with a high degree of isolation. The strong LO pulses contain more than 5×10^7 photon per pulse and the inline attenuator is used to generate the weak coherent states (WCS) signal pulses down to less than one photon per pulse on average.

Then the combined signal-LO pulses pass through a QKD link with 64 km length in a standard telecom single mode fiber (SMF). Bob uses a polarization-beam-splitter (PBS) with a polarization extinction ratio of 25 dB to separate the horizontally polarized strong LO pulses and the vertically polarized weak signal pulses. A small portion of the strong LO component is picked up for the receiver synchronization, using a PIN diode D3.

Bob's receiver has a similar Mach-Zehnder interferometer structure. He performs the LO phase shift in the upper arm on a Lithium Niobate phase modulator to apply his base choice (Φ_B: π/4 in Base B_1, -π/4 in Base B_2), constituting a BPSK conversion in which $\Phi = \Phi_A - \Phi_B$. The delay between the signal and the strong LO pulses is carefully adjusted to 20 ns to optimize the time overlap on the PM coupler's input ports with the same state of polarization (SOP).

In this BHD setup, the phase drift $\Delta\Phi$ is compensated by an optoelectronic feedback using a phase shifter (PS) in Bob's lower arm using "training frame header" so as to compute the phase drift and feedback on the PS.

8.2.2 Phase Compensation with Training Frame

In the BHD scheme, the LO level remains constant, and only the signal level is strongly attenuated with the attenuator 1. We use a balanced photo-detector (Thorlabs PDB150C-EC) in association with a passband voltage amplifier (Femto, Series DHPVA, 200 MHz) to obtain an optimized resolution for the high-speed 8-bit ADC PCI transient recorder that works at a sample rate up to 200 Mbits/s (Spectrum M2i.2030).

Four registers R_0, $R_{\pi/2}$, R_π, $R_{3\pi/2}$ store and update the estimated values for the four possible phase states. The detected values of the *M* bits are $\{a_1, a_2, \ldots, a_M\}$, in which $\{a_{i1}, a_{i2}, \ldots, a_{i(M/4)}\}$, $\{a_{j1}, a_{j2}, \ldots, a_{j(M/4)}\}$, $\{a_{m1}, a_{m2}, \ldots, a_{m(M/4)}\}$, $\{a_{n1}, a_{n2}, \ldots, a_{n(M/4)}\}$ correspond to the bits that carry phase information 0, π/2, π and 3π/2, respectively.

The normalized quadrature amplitude of the detected signal is proportional to $\cos(\Phi) = \cos(\Phi_A - \Phi_B)$. We also assume that the phase errors corresponding to each phase state are $\Delta\Phi_0$, $\Delta\Phi_{\pi/2}$, $\Delta\Phi_\pi$, $\Delta\Phi_{3\pi/2}$, respectively.

We can approximately obtain:

$$\begin{cases} R_0 = \overline{a_{ik}} = \left(\sum_{k=1}^{M/4} a_{ik}\right) \Big/ (M/4) = A_0 \cos(\Delta\Phi_0) \\ R_{\pi/2} = \overline{a_{jk}} = \left(\sum_{k=1}^{M/4} a_{jk}\right) \Big/ (M/4) = A_{\pi/2} \cos(\Delta\Phi_{\pi/2} + \pi/2) \\ R_\pi = \overline{a_{mk}} = \left(\sum_{k=1}^{M/4} a_{mk}\right) \Big/ (M/4) = A_\pi \cos(\Delta\Phi_\pi + \pi) \\ R_{3\pi/2} = \overline{a_{nk}} = \left(\sum_{k=1}^{M/4} a_{nk}\right) \Big/ (M/4) = A_{3\pi/2} \cos(\Delta\Phi_{3\pi/2} + 3\pi/2) \end{cases} \tag{8.2}$$

where A_0, $A_{\pi/2}$, A_π and $A_{3\pi/2}$ are the envelope amplitudes, and we have:

$$\begin{cases} A_0 \approx A_{\pi/2} \approx A_\pi \approx A_{3\pi/2} \\ \Delta\Phi_0 \approx \Delta\Phi_{\pi/2} \approx \Delta\Phi_\pi \approx \Delta\Phi_{3\pi/2} \end{cases} \tag{8.3}$$

We can thus obtain the estimated envelope amplitude and the phase error:

$$\begin{cases} A \cong \left[\left(R_0{}^2 + R_{\pi/2}{}^2 + R_{\pi}{}^2 + R_{3\pi/2}{}^2 \right) / 2 \right]^{1/2} \\ \Delta\Phi \cong \left(\Delta\Phi_0 + \Delta\Phi_{\pi/2} + \Delta\Phi_{\pi} + \Delta\Phi_{3\pi/2} \right) / 4 \end{cases} \tag{8.4}$$

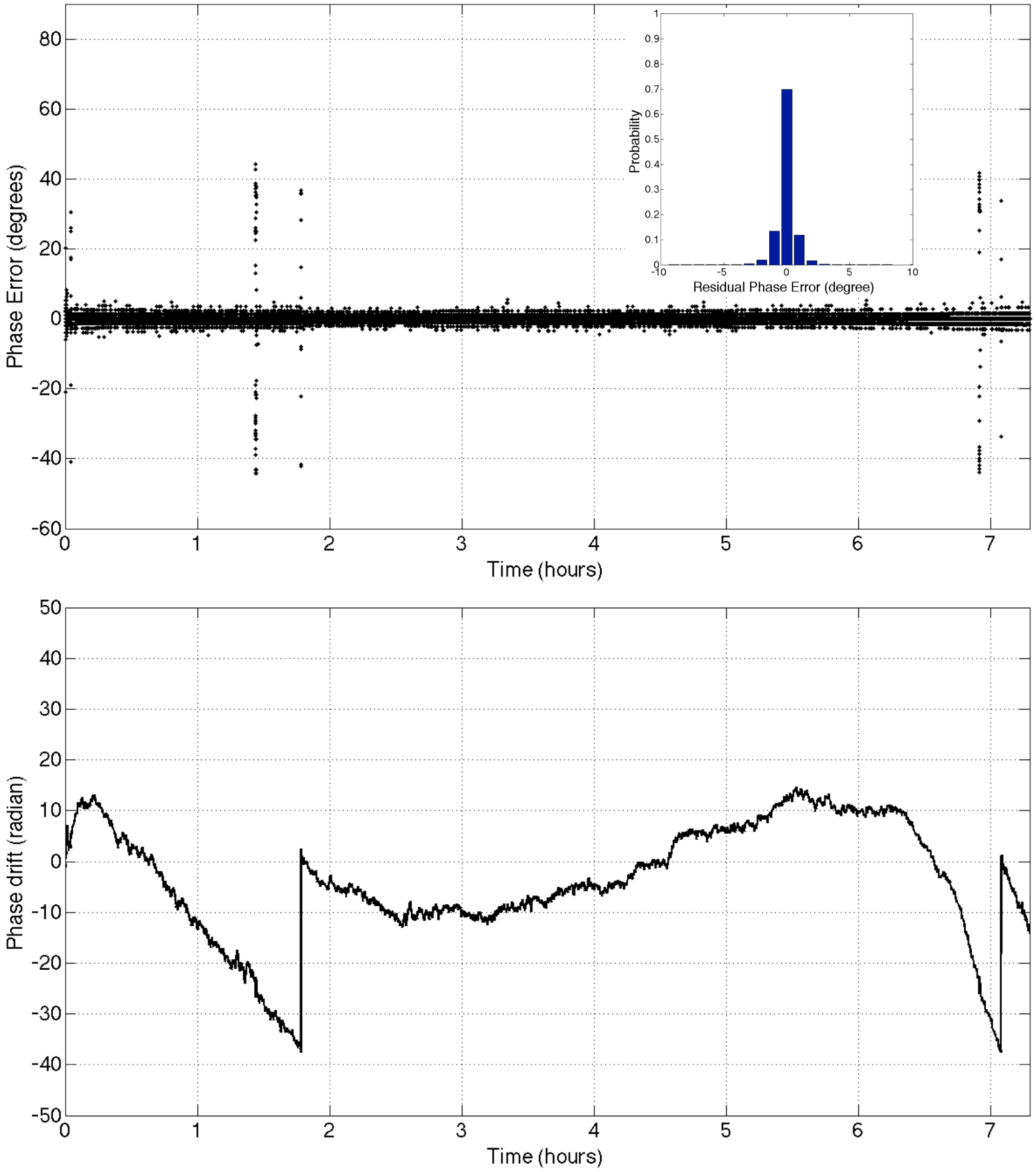


Figure 8.5 BHD QKD system residual phase error

We have taken 5% of the received bits as the “training frame header” and 95% as the “Data”. In Figure 8.5 we show the voltage applied on the phase shifter and the residual phase error for received photon number N_S = 0.8 with a minimum phase precision 1.25 degrees. The residual phase error is well controlled under 10 degrees as shown in the inset histogram in the upper figure.

8.2.3 Dual-threshold Balanced Homodyne Detection

The output of a BHD receiver is proportional to the E_S, a single quandrature of the signal corresponding to E_L and its additional quantum noise $|\Delta E_S|$. This input signal is found to be amplified by the deterministic part of the in-phase LO quadrature on the detectors that act as a noise free mixing gain. Since only one quadrature is measured, there is no additional noise to the zero-point fluctuation [9]. However, the different coherent states generated by conventional light sources are not orthogonal, leading to an inherently finite error rate and making a decision process mandatory [10-12].

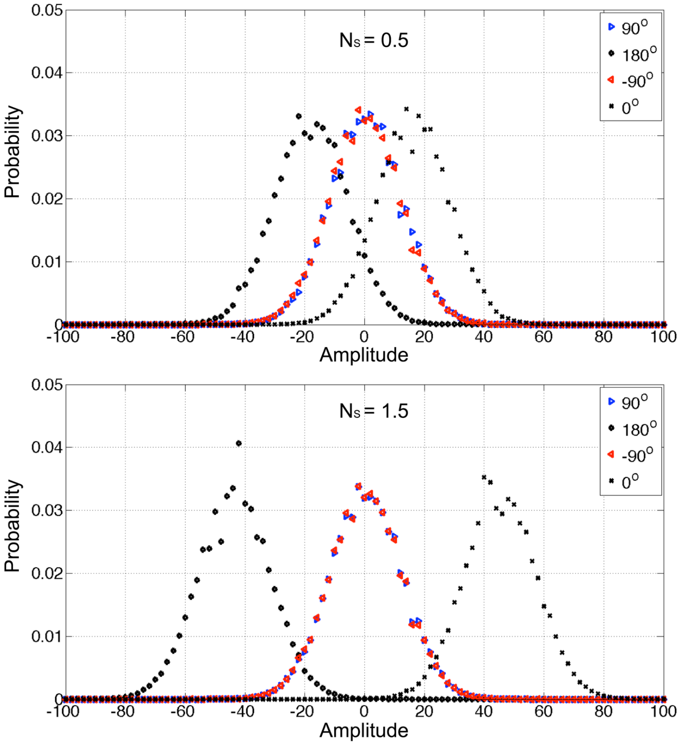


Figure 8.6 Histogram of the detected signals a) $N_S = 0.5$, a) $N_S = 1.5$

In Figure 8.6, we depict the experimental histogram (the probability density function). It is only possible to differentiate the phase states $\Phi = 0$ and $\Phi = \pi$, since the histograms of $\Phi = \pi/2$ and $\Phi = -\pi/2$ overlap with each other. Given the signal average photon number per bit N_S, the detected sum field using intensity detection in the absence of thermal noise results in the probability of error [10]:

$$BER = 1/2\, erfc\left(\sqrt{2N_S}\right) \tag{8.5}$$

where $erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty \exp\left(-t^2\right)dt$.

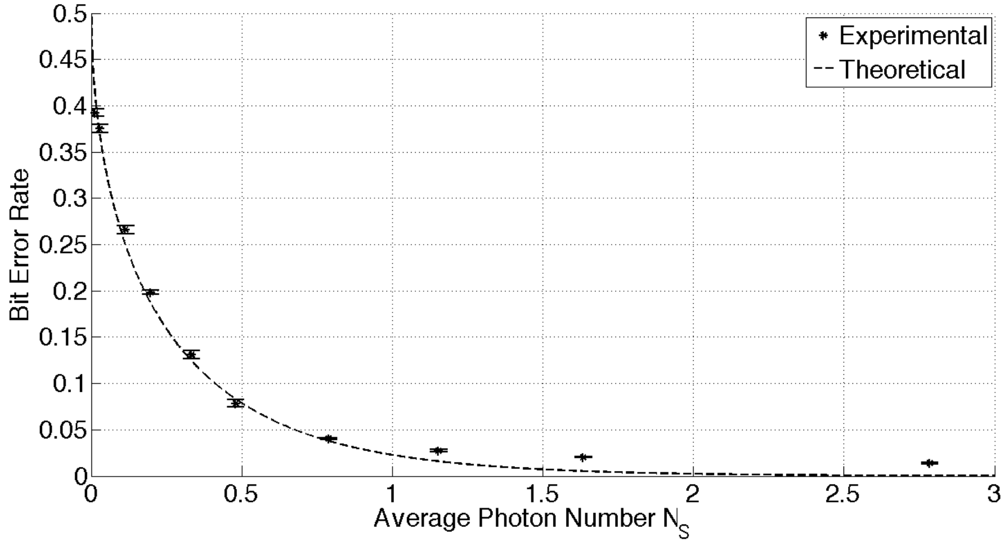


Figure 8.7 Experimental BER compared with the theoretical values

In digital communications the information loss due to the channel impairments must be processed by the forward error coding (FEC) techniques. However it differs significantly from the QKD situation in which the signal erasure (i.e. empty pulses) can be easily managed during the *a posteriori* reconciliation process [13] by a decision abandon disregarding the corresponding bits, and mainly be turned into reduction of the key generation rate. In this way BHD can also permit the accurate implementation of a dual-threshold decision process on the post-detection high-level electronic signals, allowing the possibility of inconclusive measurements to lower the BER, with a trade-off in the reduced key generation efficiency. Therefore Eve's attack turns more to a Bob's signal degradation than a substitution since the corresponding information can be suppressed during the reconciliation.

For the signal discrimination Bob sets up two symmetrical thresholds ±X (normalized to the root of the average photon number per bit $\sqrt{N_S}$) for the detected value x, with the selection rule:

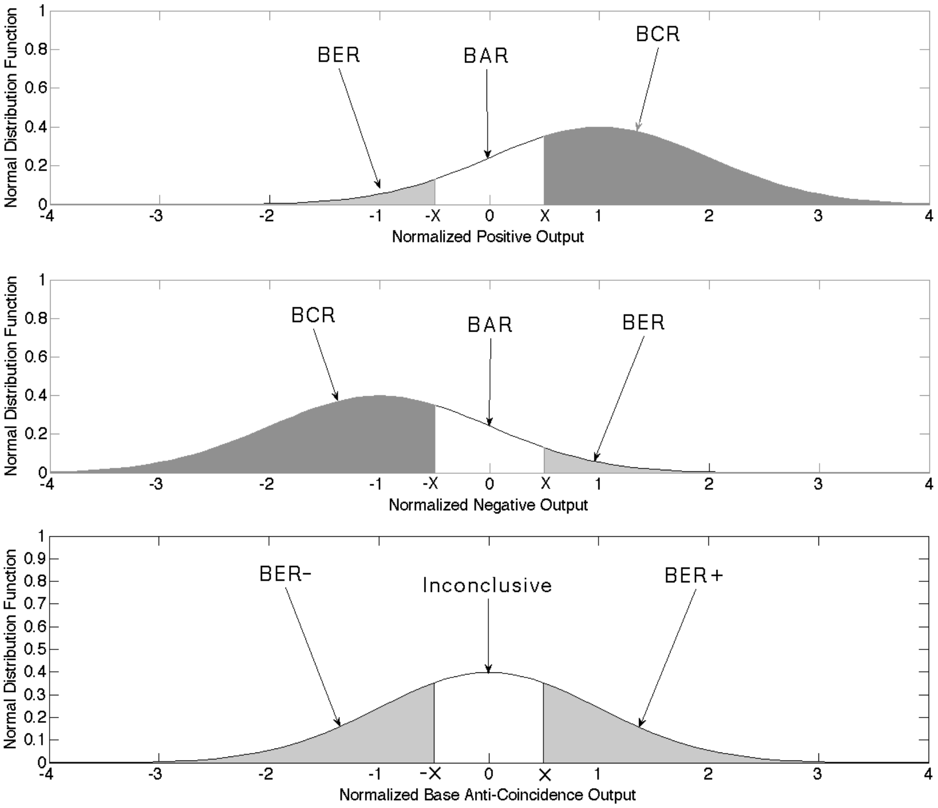


Figure 8.8 Dual-threshold BHD decision

$$Judgement = \begin{cases} 1 & if\left(x > X\right) \\ 0 & if\left(x < -X\right) \\ Abandon & otherwise \end{cases} \tag{8.6}$$

Without loss of generality we assume equal symbol probability for each phase state, thus the incoming bit error rate (BER) and the incoming bit correct rate (BCR) are given by:

$$BER_i = 1/2\,erfc\left[(2N_S)^{1/2}(X+1)\right] \tag{8.7}$$

$$BCR_i = 1/2\,erfc\left[(2N_S)^{1/2}(X-1)\right] \tag{8.8}$$

In order to dispose of a parameter to compare with photon counting, we introduce the post-detection efficiency ρ, which is defined as the probability of a conclusive judgment:

$$\rho(X,N_S) = BER_i + BCR_i \tag{8.9}$$

Also the bit abandon rate (BAR) is defined as:

$$\begin{aligned} BAR &= 1 - \rho(X,N_S) \\ &= 1 - 1/2\,erfc\left[(2N_S)^{1/2}(X+1)\right] - 1/2\,erfc\left[(2N_S)^{1/2}(X-1)\right] \\ &= erfc\left[(2N_S)^{1/2}X\right] \end{aligned} \tag{8.10}$$

In photon counting, the quantum efficiency is determined by the built-in decision circuit. For the comparison we have measured the BHD post-detection efficiency with different threshold parameters *X*, using the same experimental setup at the same repetition rate of 4 MHz. We have performed the measurements of the signal level N_S = 0.02-3.0 photons/bit with strong LO level of 2.8×10^5 photons/bit so that the quantum noise is at least 10 dB above the thermal noise.

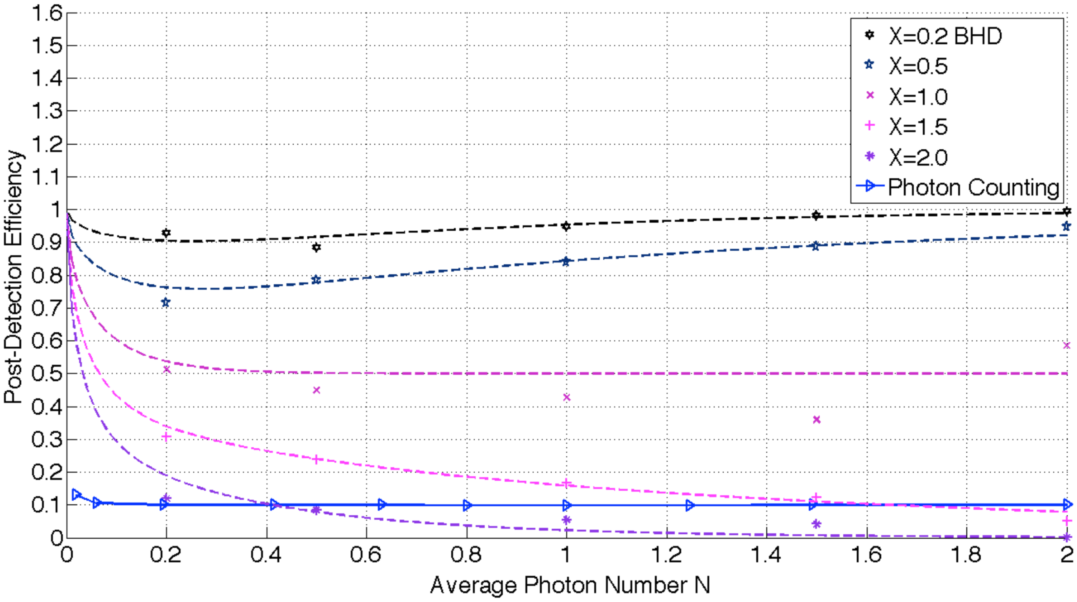


Figure 8.9 Experimental measurements of the detection efficiency

The experimental results in Figure 8.9 show that the post-detection efficiency ρ can be higher than the photon counting detection efficiency with appropriate parameters selection. As a matter of fact, even if the selection of a high threshold X decreases the detection efficiency, a high key generation rate is attainable since BHD can potentially operate at much higher speed than photon counters.

In order to compare with the QBER of photon counting, we introduce the BHD post-detection BER_P as:

$$BER_p = BER_i/\rho = (1/2\rho)erfc\left[(2N_S)^{1/2}(X+1)\right] \tag{8.11}$$

We measured the BER_P for different values of the threshold parameter X. The obtained values as shown in Figure 8.10 is slightly higher than the theoretical BER value due to the system quantification errors and other impairments such as residual polarization mismatch and modulation imprecision. (Note that when $X=0$, it is the standard single-threshold decision as depicted in Figure 8.7).

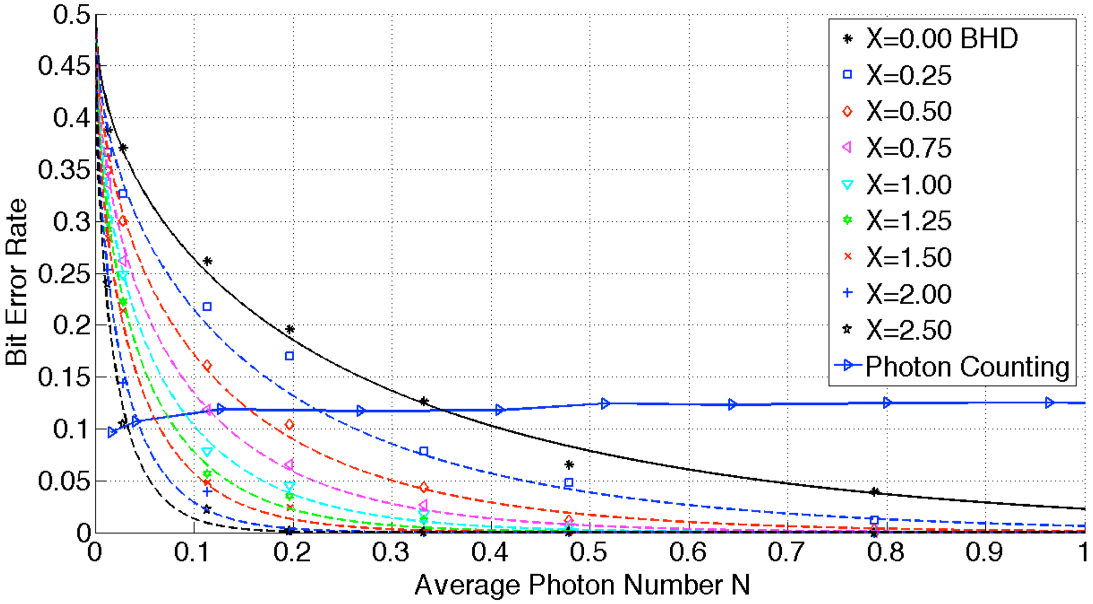


Figure 8.10 BHD post-detection BER and photon-counting QBER

The observed QBER in the PC scheme (also shown in Figure 8.10) in our phase encoding system appears higher than 0.1 due to the residual phase errors since the phase correction, calculated by counts of detected photon, is less precise than the BHD scheme as a consequence of the limited counting events, unequal PC detection efficiency, as well as the dark counts. It appears constant over a wide range of signal level since errors are mainly produced by the phase errors and the limited extinction ratio that are in principal independent of the signal level. QBER can only be improved by a more accurate phase and polarization control, such as polarization stabilizer, special pulsed laser source with narrower spectral line-width and wider coherent time, as well as higher extinction ratio optical devices. Meanwhile BHD scheme can also take advantage of these improvements, still making it a more efficient detection scheme.

Table 8-1 Photon Counting VS Dual-threshold BHD

Photon Counting	**Dual-threshold BHD**
Low speed Geiger mode APD	High speed PIN photodiodes
Low quantum efficiency< 10%	High quantum efficiency > 90 %
Equal amplitude reference	Strong reference LO
Signal independent threshold	Signal dependent threshold
Dark count limited QBER	Shot noise limited BER_P
Delicate phase synchronization	Efficient phase synchronization

In Table 8-1 we have already mentioned the different characteristics of the two receiver configurations. As a matter of fact, in PC the inherent threshold parameter is adjusted as a trade-off between quantum efficiency and dark count rate, and is independent of the received signal so as to offer a wide operation range for single photon measurements; while in BHD the dual-threshold can be more flexibly adjusted as a trade-off between BER_P and key exchange rate. Furthermore, the dual-threshold BHD scheme has three main advantages over photon counting scheme: a) the quantum efficiency of PIN photodiodes is near unity; b) ultra-high speed QKD system is achievable since no quenching process is required; c) the cost of telecom wavelength PIN photodiodes is much lower and the supply requirements are much simpler.

Recently a decoy-state protocol has been proposed [14] and extensively studied by some research groups [15-18]. The signal state intensity can be chosen to be up to one photon on average thanks to a more sophisticated reconciliation process. The BHD system is readily adaptable for such a protocol since it allows distinguishing the multi-photon coherent states.

8.3 SECURITY OF THE DUAL-THRESHOLD BHD QKD SYSTEM

In this section, we analyze the security issues of the BHD QKD system under the "intercept-resend" attack and the "intermediate base" attack, provided that the guarantee of security lies either on the mutual information gain or the perception of the eavesdroppers' intervention [8].

In order to investigate the security of a quantum cryptosystem, we have to take into account the action of Eve, and we analyze the amount of information accessible to her. We represent the information entropy of Alice by $H(A)$. The conditional entropies of Bob and Eve are defined as $H\left(A|B\right)$ and $H\left(A|E\right)$ given that Alice's information is known. The mutual information *I(A,B)*, *I(A,E)* are defined as the estimation of the information shared by Alice and Bob, and that shared by Alice and Eve, respectively. Note that Eve is supposed to be limited only by the physical laws.

$$\begin{cases} I\left(A,B\right) = H(A) - H\left(A|B\right) \\ I\left(A,E\right) = H(A) - H\left(A|E\right) \end{cases} \tag{8.12}$$

The key is said to be secure if the *I(A,B)* is higher than *I(A,E)* [19]. Therefore we define the amount of the obtainable security *S*:

$$S = I\left(A,B\right) - I\left(A,E\right) = H(A|E) - H(A|B) \tag{8.13}$$

According to information theory, if *S* is positive, it is theoretically possible to decrease the amount of information gained by Eve through the process of "privacy amplification", i.e. Alice and Bob abandon randomly a portion of the obtained key sequence to decrease Eve's useful information [20,21]. Otherwise, i.e. when *S* is negative, the key must be dropped as long as no algorithm could guarantee the unconditional security. In this case, Bob should be able to detect Eve's intervention. [22].

We have analyzed the security issues in view of two potential individual attacks, along with a mixed power attack strategy.

8.3.1 INTERCEPT-RESEND ATTACK

In order to evaluate the differential mutual information S, we calculate Bob's BER under Eve's intercept-resend attack in which she performs five main steps:

1) Eve listens to the quantum channel and steals all the Q-bits.

2) She splits the signal in two equal parts.

3) She performs a measurement of the two equal parts on the two bases (as Bob's bases); accordingly she obtains two measured values x_1 and x_2.

4) As she makes the decision, she chooses the most likely value from the two measures and resends it to Bob. For example, if $x_1 > |x_2|$, then Eve resends to Bob the bit "1" on the base A1. Nevertheless she stores the two measured values until the reconciliation process.

5) During the reconciliation process, Eve listens carefully to the divulgation of the bases used by Alice and Bob. To improve her information, she switches those wrong decisions made in step 3.

Namiki and Hirano [23] have given some specific contributions with respect to Eve's intervention analysis. We define P_+ as the probability that Eve resends the correct bit state on the correct base:

$$\mathrm{P}_+ = \frac{1}{4}\left(\mathrm{erfc}\left(-\left(N_S/2\right)^{1/2}\right)\right)^2 \tag{8.14}$$

P_- as the probability that Eve resends the wrong bit state on the correct base:

$$\mathrm{P}_- = \frac{1}{4}\left(\mathrm{erfc}\left(\left(N_S/2\right)^{1/2}\right)\right)^2 \tag{8.15}$$

and $\mathrm{P}_\perp$ as the probability that Eve resends the bit state on the wrong base:

$$\mathrm{P}_{\perp} = \frac{1}{4}\mathrm{erfc}\left(\left(N_S/2\right)^{1/2}\right)\mathrm{erfc}\left(-\left(N_S/2\right)^{1/2}\right) \tag{8.16}$$

Hence the modified post-detection efficiency and the modified BER at Bob's end:

$$\rho'\left(X,N_s\right) = \left(\mathrm{P}_{+}(N_s) + \mathrm{P}_{-}(N_s)\right)\rho(X,N_s) + 2\mathrm{P}_{\perp}\,\mathrm{erfc}\left(\left(2N_S\right)^{1/2}X\right) \tag{8.17}$$

$$BER_{Bob}'\left(X,N_s\right) = \frac{\mathrm{P}_{+}(N_s)BER_i + \mathrm{P}_{-}(N_s)BCR_i + \mathrm{P}_{\perp}(N_s)\mathrm{erfc}\left(\left(2N_S\right)^{1/2}X\right)}{\rho'\left(X,N_s\right)} \tag{8.18}$$

Eve's BER can simply be obtained as if she performs the measures on half the signal power, hence $BER_{Eve}' = BER_i(0,N_s/2) = 1/2\cdot erf\,c\left(\sqrt{N_S}\right)$.

As we have mentioned in equation (8.13), we can obtain the differential mutual information by calculating Alice-Bob, and Alice-Eve mutual information:

$$\begin{cases} H(A|B)' = -\left(BER_{Bob}'\log_2\left(BER_{Bob}'\right) + \left(1 - BER_{Bob}'\right)\log_2\left(1 - BER_{Bob}'\right)\right) \\ H(A|E)' = -\left(BER_{Eve}'\log_2\left(BER_{Eve}'\right) + \left(1 - BER_{Eve}'\right)\log_2\left(1 - BER_{Eve}'\right)\right) \end{cases} \tag{8.19}$$

And we can obtain the differential mutual information $S' = H(A|E)' - H(A|B)'$.

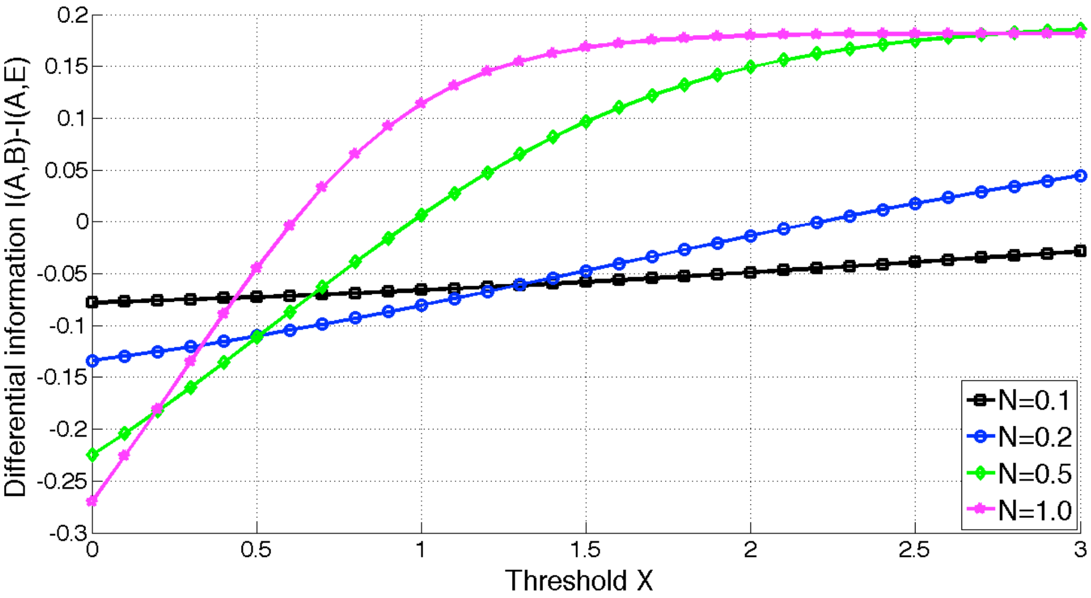


Figure 8.11 The differential mutual information under intercept resend

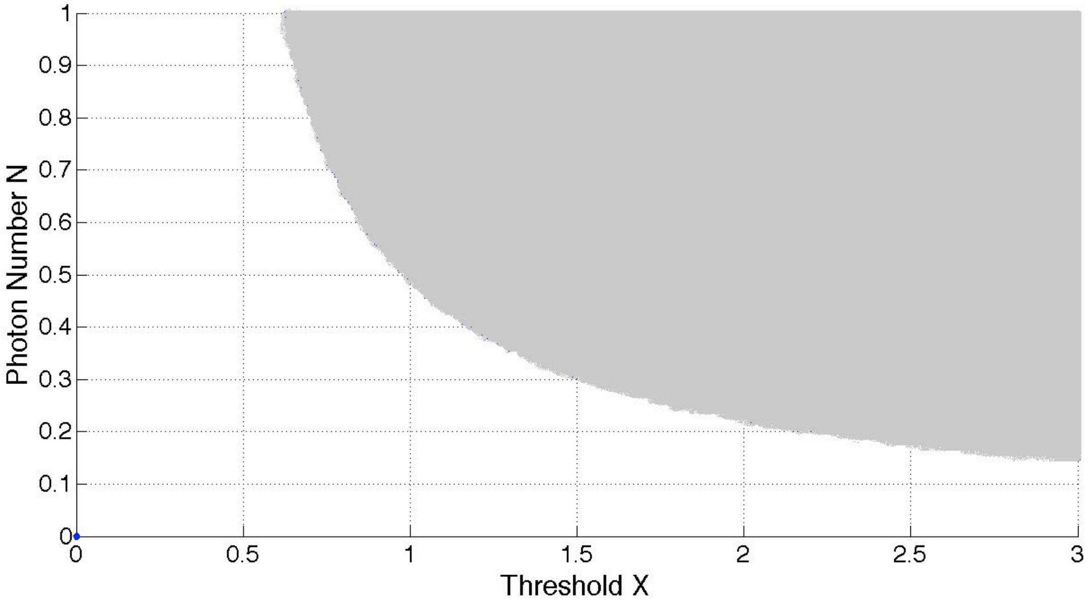


Figure 8.12 The security zone under intercept-resend attacks

As a higher threshold X could allow Bob to obtain a lower BER, we conclude that with appropriate parameters (X, N_S) Alice and Bob can guarantee the unconditional security wherever the differential mutual information S is above 0 as shown in Figure 8.12.

8.3.2 Intermediate Base Attack

In the intermediate base attack Eve performs the four main steps:

1) Eve steals all the Q-bits.

2) She performs the measurements of all the Q-bits with the intermediate base $\Phi = \pi/4$.

3) She resends to Bob the bits she has obtained on the intermediate base, and stores the bit values until the reconciliation process.

4) During the reconciliation process, she uses the base revelation to discriminate the bit states (0 or 1) that Alice has sent.

The loss of Eve in the step 2 is 3 dB due to the intermediate base projection. Thus Eve's BER is the same as under the intercept-resend attack. Furthermore we can deduce from equations (8.7), (8.8) that

$$BER_{Eve}'' = BER_i(0, N_s/2) = 1/2\, erfc\left[\left(N_S\right)^{1/2}\right] \tag{8.20}$$

and Eve's BCR is:

$$BCR_{Eve}'' = BCR_i(0, N_s/2) = 1/2\, erfc\left[-\left(N_S\right)^{1/2}\right] \tag{8.21}$$

Consequently Bob's incoming BER and BCR are modified:

$$BER_i'' = BER_i\left(X, N_S/2\right) = 1/2\, erfc\left[\left(N_S\right)^{1/2}\left(X+1\right)\right] \tag{8.22}$$

and Bob's BCR is:

$$BCR_i'' = BCR_i\left(X, N_S/2\right) = 1/2\, erfc\left[\left(N_S\right)^{1/2}\left(X-1\right)\right] \tag{8.23}$$

And Bob's modified efficiency is given by

$$\rho''(X, N_s) = BER_i'' + BCR_i'' = \rho(X, N_s/2) \tag{8.24}$$

Thus the modified Bob's BER is given by:

$$BER_{Bob}''(X,N_s) = \frac{BER_{Eve}''BCR_i''+BCR_{Eve}''BER_i''}{\rho''(X,N_s)} \tag{8.25}$$

We can obtain in the very same way, the differential mutual information by calculating Alice-Bob, and Alice-Eve mutual information:

$$\begin{cases} H(A|B)'' = -\left(BER_{Bob}''\log_2(BER_{Bob}'') + (1-BER_{Bob}'')\log_2(1-BER_{Bob}'')\right) \\ H(A|E)'' = -\left(BER_{Eve}''\log_2(BER_{Eve}'') + (1-BER_{Eve}'')\log_2(1-BER_{Eve}'')\right) \end{cases} \tag{8.26}$$

Therefore the differential mutual information by calculating Alice-Bob, Alice-Eve mutual information, and $S'' = H(A|E)'' - H(A|B)''$.

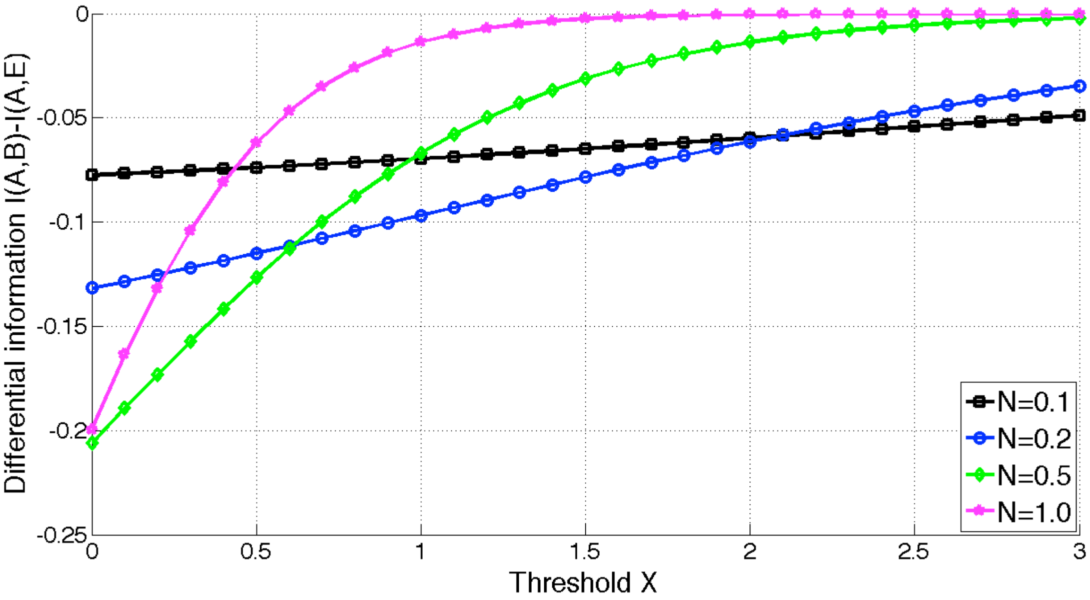


Figure 8.13 The differential mutual information under intermediate base attack

Figure 8.13 shows that Eve could always obtain more information than Bob, thus this quantum link is not unconditionally secure under the intermediate base attack. Therefore, Bob must be capable of detecting the Eve's intervention and tell Alice.

In Figure 8.14 we give the theoretical comparison of the post-detection BER evaluation when $X \in \{0, 1.0, 2.0\}$ are used: the BER is largely modified under the two attacks. When we chose to use a higher threshold X, it will be more evident to discern Eve's attacks by comparing the operating post-detection BER with the original post-detection BER.

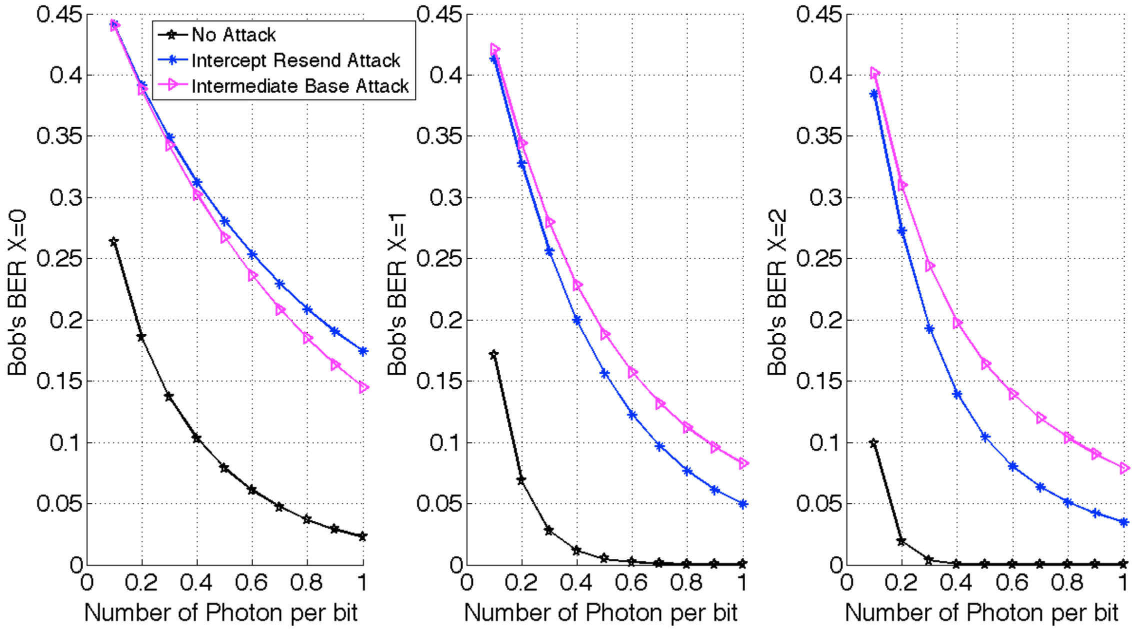


Figure 8.14 The post-detection BER evaluations with different $X = 0, X = 1, X = 2$

8.3.3 Attacks and Power Analysis

It has been proven in the precedent chapters that Eve could not obtain useful information by using the two types of attack, in that when she gains more mutual information than Bob, the key will be discarded. Now we investigate on Eve's mixed attack strategy: using power modification to hide her intervention.

As Eve makes the decisions and resends the key sequence to Bob, she can actually modify the signal power so as to circumvent Bob's vigilance. She will seek to lower *I(A,B)* and maintain Bob's post-detection BER to conceal her attacks. In this regard, we replaced the signal level N_S by βN_S (β is a power factor to account for Eve's intention). If

Eve resends the signal at the same power level as she has received, $\beta = 1$. If $\beta > 1$ she amplifies the signal power and if $\beta < 1$ she resends the signal bit with attenuation.

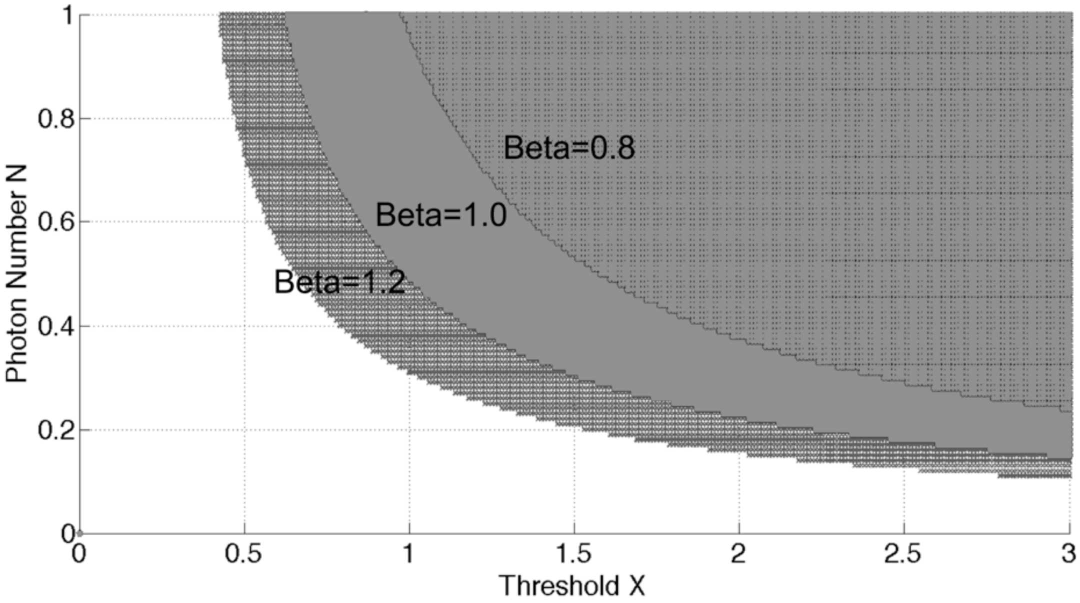


Figure 8.15 The security zone under intercept resend attacks with different β

We illustrate the security zone under the intercept-resend attack in Figure 8.15 for $\beta \in \{0.8;1;1.2\}$. Secure zone stands for positive differential mutual information *S*. First we can see that amplifying the signal will not be a wise choice for Eve, since doing so she lowers Bob's post-detection BER but increases *I(A,B)*, as well as a larger security zone. In the other hand, if she attenuates the signal, Bob will be aware of her presence since the incoming BER_i will increase and the detection efficiency will drop in consequence.

Under the intermediate base attack, if Eve amplifies the signal power, Bob will also have a lower post-detection BER, however this β has to be very high to hide her presence. In this case, by comparing the incoming BER_i, the detection efficiency and the post-detection BER, Bob can still find out that Eve has been attacking the quantum channel. And if she attenuates the signal, the increasing post-detection BER and incoming *BER_i*, together with the decreasing detection efficiency will reveal her presence.

In conclusion, Eve's mixed strategies can be diversified, i.e., independent attacks including individual and collective attacks, or joint attacks in which multiple attacks coexist in the quantum channel. However, if she doesn't manage to gain the mutual information and maintain Bob's incoming *BER_i* and post-detection *BER* to cover up her action at the same time, the attack will be discerned.

At Bob's side, in order to guarantee the security he needs to set a high threshold so as to lower the incoming *BER_i* and the post-detection BER to make Eve's intervention detectable. This is consistent with the parameters choice of a higher performance system thanks to BHD's high potential operation rates.

8.3.4 Long Distance Standard Transmission

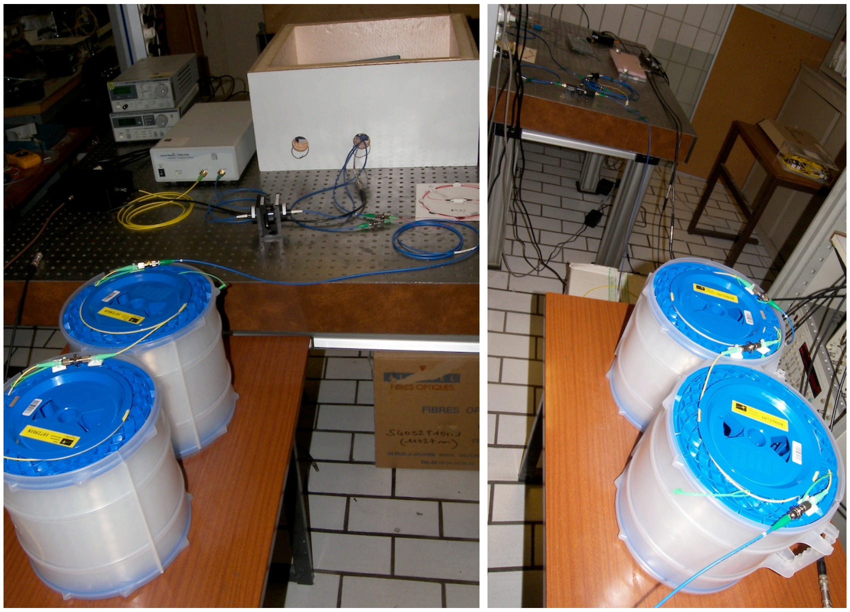


Figure 8.16 QKD long distance transmission a) Alice's side; b) Bob's side

Long distance transmission in optical fiber is subject to impairments such as fiber loss of 0.2 dB/km and dispersion of 17 ps/km•nm at 1550 nm wavelength, which are the issues that a QKD system has to overcome in a practical and constant field operation.

We have performed the experiments [24] with strong LO pulses containing more than 5×10^7 photons, and the inline attenuator is used to adjust the weak signal pulses to mean energy below 1 photon, with a repetition rate of 16 MHz. We have successfully evaluated the system performance with SMF links of 0 km, 25 km, 50 km and 64 km with different threshold parameters X: 0, 0.5, 1 and 2.

In Figure 8.17 we show the experimental post-detection BER_P as compared to the theoretical values. The measured BER_P is slightly higher than the theoretical values due to the connection loss, residual phase fluctuations, and the quantification errors issued from the 8-bit A/D converter. Indeed the LO pulses attenuate meanwhile with the weak signal pulses in the SMF link, e.g. at 64 km we have measured a transmission loss of 16.5 dB, i.e. the signal mean photon number $N_S = 0.0224$, and in principle the quantum noise is lower than the thermal noise from 90 km. Hence setting a higher dual-threshold is necessary and beneficial to obtain its optimal throughput as a tradeoff in the effective key generation rates, which is still much higher than that of SPDM since BHD can operate at very high frequency thanks to the PIN photodiodes. However the effective transmission limit is bounded by the QBER security limit 11% [25], e.g. at around 50 km when $X = 2$.

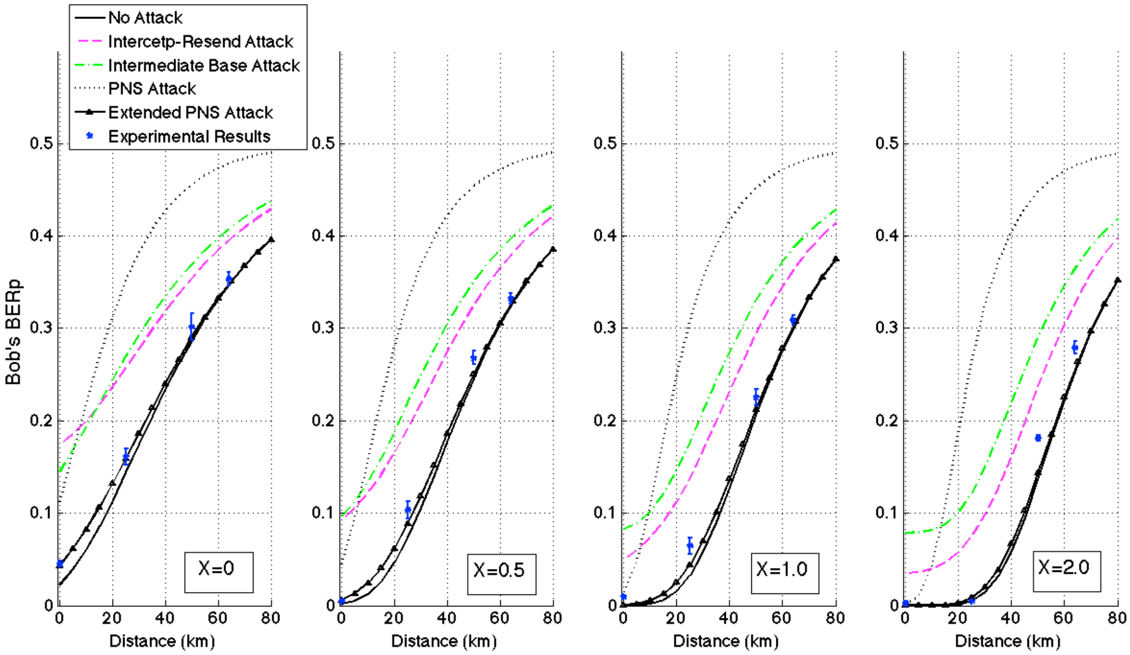


Figure 8.17 Bob's Post-detection BER over different distances of transmission

In Figure 8.17 we also give the theoretical evaluation of the post-detection BER_P using different threshold values X: the BER_P is largely modified under the intercept-resend, intermediate base and PNS attacks [26]. As we have already discussed before, under intercept-resend attack Bob can select a higher X value to maintain the information gain over Eve, while no information gain can be obtained under intermediate base and PNS attacks. In this case Bob can discern Eve's attacks by comparing the operating BER_P with the theoretical BER_P at the receiver's Bob end. Under the more advanced extended PNS (Ex-PNS) attack proposed by Lütkenhaus [27] in which Eve hides her presence by stealing only multi-photon pulses, a multi-states protocol similar to decoy states can be used to observe the detection efficiency ρ variations using higher photon number pulses and single photon pulses.

As the coherent laser pulses follow the Poisson distribution, we can easily observe the statistics variations under Eve's Ex-PNS attack, as shown in the Fig 8.18. Bob can identify Eve's attack by implementing a multi-states protocol containing pulses of varying average power. The weak pulses containing less than 1.0 photon/bit, i.e. the signal states, should be used for the key generation; while the stronger pulses, i.e., the decoy states, should be used for the statistics evaluation of the received signal. The positions of decoy states and signal states are predetermined between Alice and Bob, thus unknown to Eve. Therefore Eve can only apply her attack strategy to every bit by stealing one photon from multi-photon pulses.

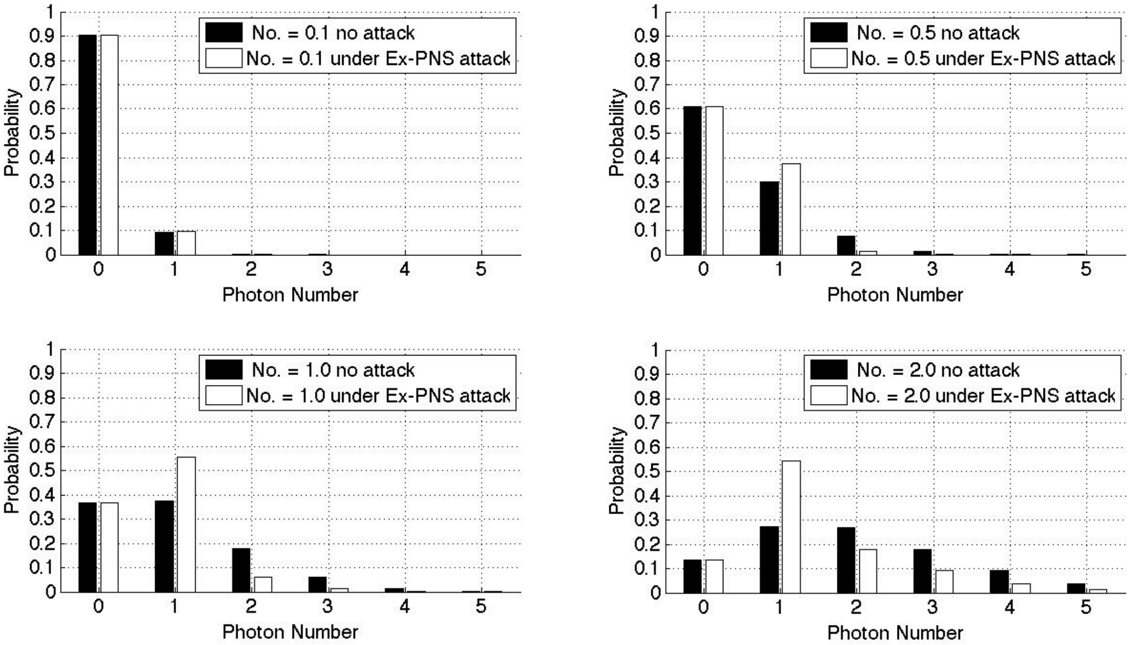


Figure 8.18 Bob's Post-detection photon number statistics under the Ex-PNS attack

By using the BHD receiver, Bob can also measure the mean values of the base-coincidence phase states for both the signal pulses and the decoy pulses, separately, to identify Eve's attacks. Furthermore, to conceal the usage of decoys states, Alice and Bob can envisage two or more different decoy states levels. As a matter of fact, the decoy states can be implemented in the intervals of training frames, since the relatively higher-level signal can not only facilitate the phase compensation loop, but also make the statistics evaluation easier.

REFERENCES

1. H. P. Yuen, and V. W. S. Chan, “Noise in homodyne and heterodyne detection”, *Optics Letters* **8**, 177--179 (1983).
2. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection”, *Physical Review A* **68**, 042331 (2003).
3. J. R. Barry, and E. A. Lee, “Performance of coherent optical receivers”, *Proceedings of IEEE* **78**, 1369--1393 (1990).
4. Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, “One way differential QPSK quantum key with channel impairment compensation”, *CLEO/Europe-IQEC*, JSI-3 (2007).
5. Q. Xu, M. B. Costa e Silva, P. Gallion, and F. Mendieta, “Auto-compensating quantum Crypto-system using homodyne detection”, *Optical Fiber Communication Conference, OFC 2008*, JWA49 (San Diego, California, 2008).
6. Id Quantique, “Single-photon detection with InGaAs/InP avalanche photodetectors”, *Single-Photon detector Module: Application note, http://www.idquantique.com*.
7. MagiQ Technologies, Inc., *“MagiQ quantum cryptography test bed: uncompromising research results”, http://www.magiqtech.com*, (2005).
8. Q. Xu, M. Sabban, M. B. Costa e Silva, P. Gallion and F. J. Mendieta, “Dual-threshold balanced homodyne detection in 1550nm optical fiber quantum cryptography system”, to be published in IEEE/OSA Journal of Lightwave Technology (2009).

9. S. Machida, Y. Yamamoto. “Quantum-limited operation of balanced mixer homodyne and heterodyne receivers”, *IEEE Journal of Quantum Electronics* **22**, 617--624 (1986).
10. C. W. Helstrom, *Quantum Detection and Estimation Theory, Mathematics in science and Engineering* **123**, (New York: Academic Press, 1976).
11. J. G. Webb, T. C. Ralph and E. H. Huntington, “Homodyne measurement of the average photon number”, *Physical Review A* **73**, 033808 (2006).
12. R. L. Cook, P. J. Martin, and J. M. Geremia, “Optical coherent state discrimination using a real-time closed-loop quantum measurement”, *Nature* **446***,* 774-777 (2007).
13. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, “Quantum cryptography using pulsed homodyne detection”, *Physical Review A* **68**, 042331 (2003).
14. W.-Y. Hwang, “Quantum key distribution with high loss: toward global secure communication”, *Physical Review Letters* **91**, 057901 (2003).
15. X.-F. Ma, B. Qi, Y. Zhao, and H-K. Lo, “Practical decoy state for quantum key distribution”, *Physical Review A* **72**, 012326 (2005).
16. X.-B. Wang, “Beating the photon pulse-number-splitting attack in practical quantum cryptography”, *Physical Review Letters* **94**, 230503 (2005).
17. H.-K. Lo, “Decoy state quantum key distribution”, *Physical Review Letters* **94**, 230504 (2005).
18. D. Rosenberg, “Long-distance decoy-state quantum key distribution in optical fiber”, *Physical Review Letters* **98**, 010503 (2007).

19. C. E. Shannon, “A mathematical theory of communication”, *Bell System Technical Journal* **27**, 379--423 and 623--656 (1948).

20. C. H. Bennett, G. Brassard, J-M. Robert, “Privacy amplification by public discussion”, *SIAM Journal on Computing* **17**, 1919--1923 (1988).

21. C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer, “Generalized privacy amplification”, *IEEE Transactions on Information Theory* **41**, 1915--1923 (1995).

22. M. Koashi, “Unconditional security of coherent state quantum key distribution with a strong reference phase pulse”, *Physical Review Letters* **93**, 120501 (2004).

23. R. Namiki, and T. Hirano, “Security of quantum cryptography using balanced homodyne detection”, *Physical Review A* **67**, 022308 (2003).

24. Q. Xu, M. Sabban, and P. Gallion, “Homodyne Detection of Weak Coherent Optical Pulse: Applications to Quantum Cryptography”, to be published in *Microwave and Optical Technology Letters Volume* (2009).

25. P. W. Shor, and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, *Physical Review Letters* **85**, 441--444 (2000).

26. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on Practical Quantum Cryptography”, *Physical Review Letter* **85**, 1330 (2000).

27. N. Lütkenhaus, and M. Jahma, “Quantum Key Distribution with Realistic States: Photon-number Statistics in the Photon-number Splitting Attack”, *New Journal of Physics* **4**, 44 (2002).

CHAPTER 9 WEAK COHERENT STATES HOMODYNE COMMUNICATIONS WITH OPTICAL PHASE SYNCHRONIZATION

Coherent detection technique [1-6] is also appearing in various new telecommunication applications working with photon numbers per bit substantially lower than those used in direct detection communications [7-10], due to its unique advantage of the noise free mixing gain, provided by the local oscillator allowing to overcome the high level thermal noise. In a quantum channel, information symbols are a set of states at quantum level encoded into complex amplitude [11] that must be discriminated at the receiver end, in the presence of channel impairments [12-14]. In this chapter we introduce the implementation of a synchronized feedback homodyne detection system for weak coherent states by minimizing the real-time phase error, using a digitalized Costas loop conducting sequential in-phase and quadrature measurements. This receiver configuration leads to a new effective method of high-speed homodyne communications by overcoming the 3 dB penalty compared to simultaneous measurements, especially for suppressed carrier communications in both the synchronization and the demodulation stages, at the price of a reduction on effective bit rate. We also introduce a new method for the Wigner function reconstruction from quadrature measurements using 128 equidistant phase states from 0 to 2π.

9.1 WEAK COHERENT STATES HOMODYNE COMMUNICATIONS

Coherent optical fiber communications have raised increasing interests [1-4] due to the possible use of complex amplitude modulations that allows lower optical signal-to-noise ratio (OSNR) for a given post-detection bit-error-rate (BER), as well as a better spectral efficiency and more efficient modulation schemes. Balanced receiver configuration using PIN photodiodes, facilitated by a strong local oscillator (LO) whose noise has only negligible influence [5], measures only one quadrature and there is no additional noise to the zero-point fluctuation of the signal field. Therefore the output noise is dominated only by vacuum fluctuation entering in the signal port and a standard quantum limited (SQL) reception is attainable. Furthermore, the use of constant envelope formats, in opposition to the traditional intensity modulation with direct detection, is more tolerant to the non-linear impairments in the fiber [6].

Weak coherent states (WCS) are widely used in the new coherent optical applications, such as quantum cryptography [7-8], long distance free space communications [9], and highly sensitive homodyne tomography [10]. Optimal quantum receivers have been studied for digital signal detection [15-17] to discriminate the different states, and the generally used criterion is to minimize the bit error rate (BER) at a give signal level.

Coherent optical systems have to tackle the unavoidable impairments caused by the phase and polarization drift, as the dynamic fluctuations can drastically affect the performance of the demodulation process. Since homodyne detection only provides a measurement of the single signal quadrature corresponding to the LO field [19], the receiver must previously perform accurate synchronization of the optical carrier [20,21] to combat the optical signal phase fluctuations.

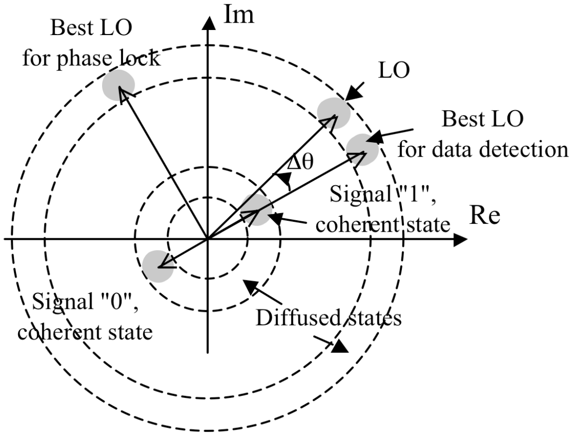


Figure 9.1 Homodyne I-Q Measurements where $\Delta\theta$ is the phase mismatch

In the classical optical coherent communication systems, the phase estimation is done in synchronizing structures such as the phase-locked-loop (PLL), using the mixing of the optical information signal with a strong optical LO [22-24]. For efficient transmission, suppressed carrier modulation such as symmetrical PSK format and Costas loop are required [25]. This loop is based on the simultaneous measurements of the received I-Q fields, as well as subsequent processing of these two results and a feedback on the LO to correct its phase, i.e. to force its phase mismatch $\Delta\theta$ to 0, as we show in Figure 9.1. However, in the quantum optical channel the simultaneous in-phase and quadrature (I-Q) measurements cannot be performed without additional 3 dB signal power penalty since it has to be divided into two parts, and the stabilization of the 90° hybrids devices is a difficult task [26,27], we thus propose a technique that performs sequential I-Q measurements of WCS using a single BHD receiver by alternatively switching [28] the phase of the LO field.

9.2 PHASE SYNCHRONIZATION WITH I-Q MEASUREMENTS

9.2.1 SYSTEM SETUP FOR SEQUENTIAL I-Q MEASUREMENTS

We implement an experimental setup [29,30] that generates and detects WCS pulses with antipodal BPSK modulation, as shown in Figure 9.1. We use a 1550 nm wavelength pulsed laser as the optical source. The beam is divided by a polarization splitting coupler (PSC) to generate in the upper arm a BPSK-modulated WCS signal using an optical phase modulator; and in the lower arm, a LO to be used for the detection and demodulation process.

In this setup, each BPSK signal is repeated to generate two identical pulses I, Q, so as to beat with the LO pulses with 0, $\pi/2$ phase switching, respectively. The WCS signal and phase-switched LO are then mixed and detected using a BHD receiver. Only the I measurements are retained and stored as data, while both the I and Q measurements are applied for the digital synthetic Costas loop processing.

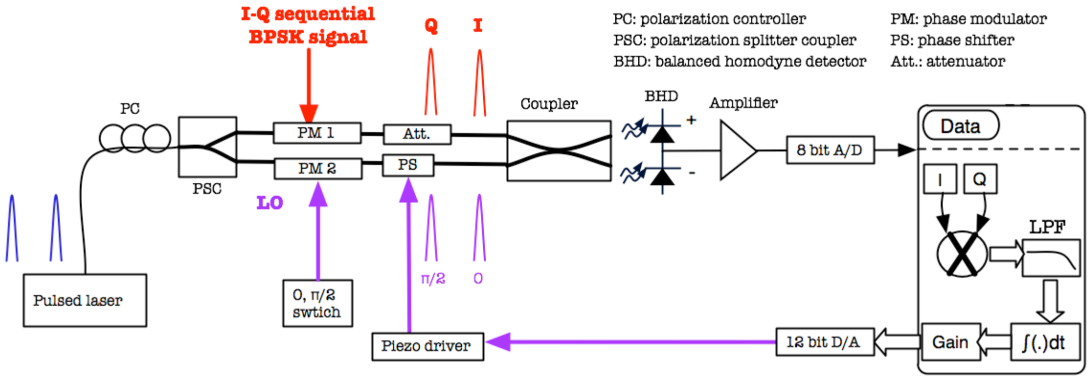


Figure 9.2 Experimental setup of the WCS sequential I-Q measurements.

The subsequent elements of the phase detection process are implemented in a discrete time mode, using an A/D converter and through a PC-based algorithm to process the raw data. This optical Costas loop is a simplified version of the maximum-a-posteriori probability (MAP) BPSK signals phase estimator [21] suggested in [22-24] for the classical channel with suppressed carrier.

9.2.2 Digital Costas Loop

In a conventional Costas loop, an error signal is generated to control the phase of an optical voltage-controlled oscillator (VCO), in our self-homodyne configuration we use an optical phase shifter (PS) to continuously synchronize the phase of the LO arm. It is important to note that the I and Q optical components are not available at the same time but that they are sent sequentially in an alternate way, and a time delay is required in order to perform the multiplication of both components before the digital Costas loop processing. In this synthetic loop, we incorporate an equivalent phase integration function of the optical VCO using an additional discrete time integrator. The resultant phase error variable is fed back via a piezo-driver on the PS to compensate for the LO relative phase drift.

The dynamics of the digital Costas loop is essentially governed by the response time of the low-pass filters used in the loop. When operating with optical signals, we design the feedback by taking into account the stochastic perturbations due to the photo-detection noise and the optical phase fluctuations. We use the following system parameters: the BPSK signal and the LO optical powers P_S, P_{LO} respectively, the raw symbol interval T_S, the signal bit interval $T_R = T_S/2$, the laser pulse width T_P, the RF amplifier gain A after the BHD receiver, the laser linewidth $\Delta\nu$, and a gain factor G after the integrator. For the implementation of the digital Costas loop, we work with the discrete-time equations as shown below:

a) The low-pass filters z-domain transfer function: $F_{LPF}(z) = \dfrac{B + Cz^{-1}}{1 - z^{-1}}$, where the constants B and C are defined as: $B = \dfrac{T_S + 2\delta_2}{2\delta_1}$, $C = \dfrac{T_S - 2\delta_2}{2\delta_1}$, with the parameters δ_1, δ_2, and N_S defined as: $\delta_1 = \dfrac{3}{8}\dfrac{T_R P_S P_{LO} A^2 G}{\pi N_R \Delta\nu}$, $\delta_2 = \left(\dfrac{4\pi}{3} \cdot \dfrac{\Delta\nu \cdot N_S}{T_R}\right)^{-1/2}$, and $N_S = \dfrac{P_S T_P}{h\nu}$.

b) The integrator z-domain transfer function: $F_{INT}(z) = \dfrac{T_S}{2}\dfrac{1 + z^{-1}}{1 - z^{-1}}$.

9.2.3 Experimental Results

We use a 1550 nm ILM light source to generate laser pulses of 5 ns at 8 MHz repetition rate. The WCS signal pulses and the strong LO pulses are polarization-aligned in a Mach-Zehnder interferometer constructed by polarization maintaining fibers. BPSK modulation on the WCS signal pulses with average signal photon number N_S is produced by an electro-optical modulator and an inline attenuator.

The I and Q components of the pseudo-random sequence are alternatively detected and the A/D and the D/A converters are used to interface the optical and the electronic subsystems. The piezo-driver delivers a wide voltage range [-10V, 150V] required for the optical PS whose half wavelength voltage V_π is 9.95 V, to obtain an operational range of [-8π, 8π] without reset, and a response time of several milliseconds. However in practice, the frequency response is limited to 1 kHz by the piezo-driver. As the system phase drift is a slow phenomenon, we update the voltage output to be applied on the PS once every 0.1 second, and the applied voltage values correspond to the mean phase error during the latest 0.1 second interval, therefore the feedback should have negligible impact on the quantum states dynamics.

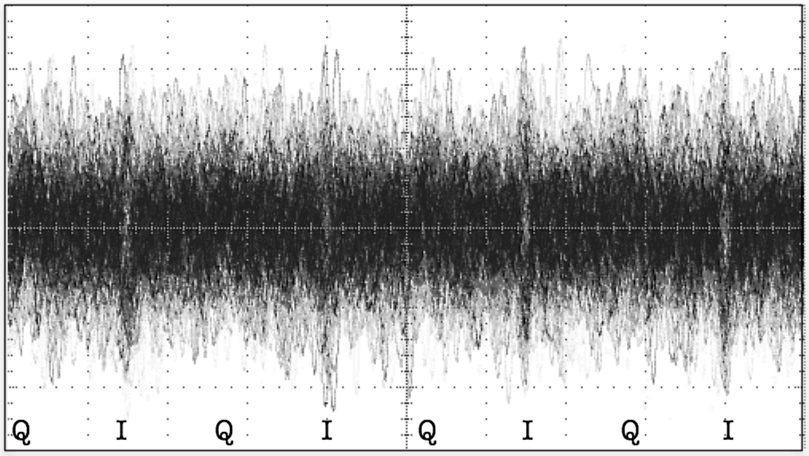


Figure 9.3 Detected signal with phase synchronization

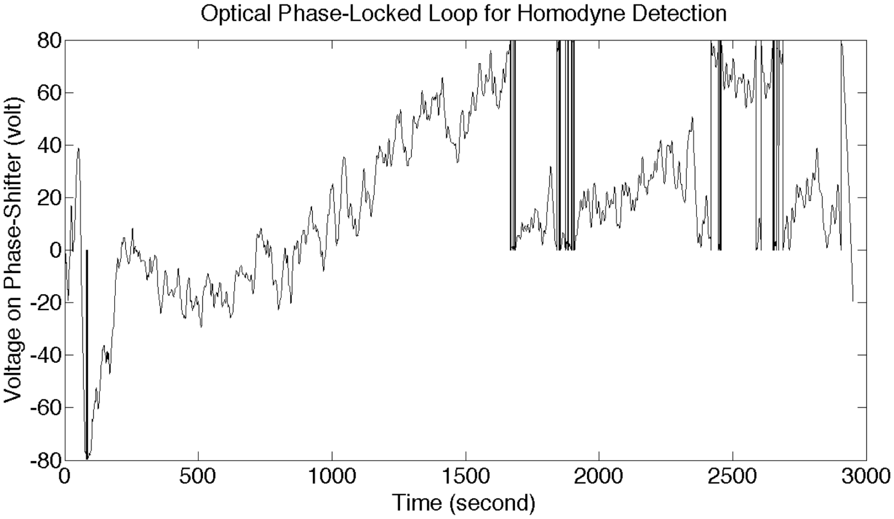


Figure 9.4 Interferometer phase tracking using digital Costas loop

We show in Figure 9.3 the detected weak signal and in Figure 9.4 the voltage applied on the PS for duration of one hour. When the phase drift reaches to the limits of the piezo-driver, our software reset the PS “zero” point so as to permit a continuous operation.

9.3 UNCERTAINTY WITH I-Q MEASUREMENTS

We have measured the BPSK signals of average photon number per pulse from 0.1 to 3 beating with the strong LO pulses of more than 4 × 10^6 photons. The normalized standard deviations for the I and Q fields measurements are bounded by the Heisenberg uncertainty principle $\Delta X_I \Delta X_Q \geq \frac{1}{4}$ (Cf. Appendix D), where ΔX_I and ΔX_Q are the normalized standard deviations of the I and Q fields.

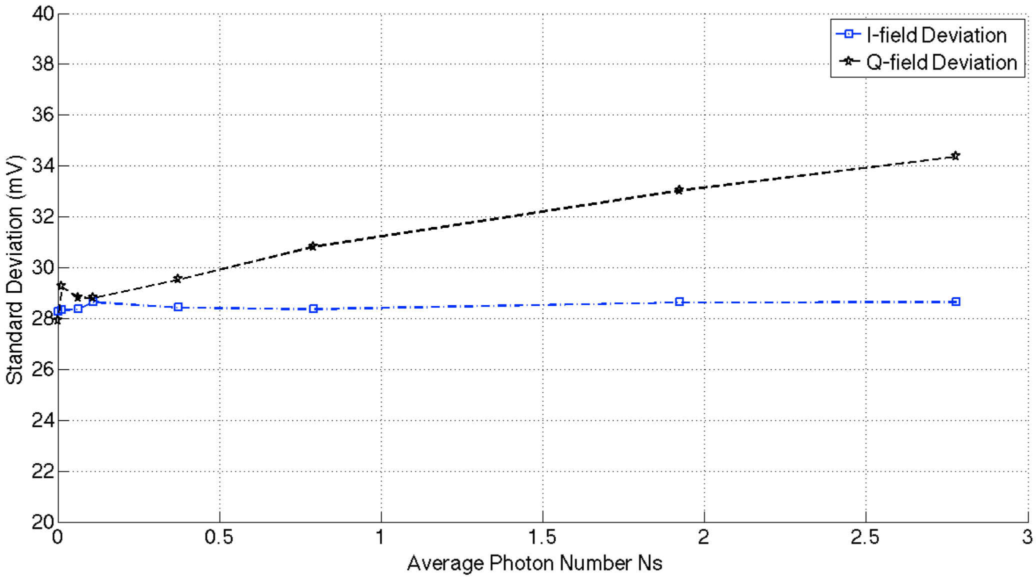


Figure 9.5 Standard deviations of the measured I, Q fields

The normalized standard deviations increase with N_S due to the excess noise compared to the vacuum fluctuations, as we show in Figure 9.5. The values have been normalized to the amplitude of the signal power N_S = 1.0. These impairments are caused by the imperfect laser source used in our experiments that does not generate perfect coherent states, the residual polarization mismatch, the imperfect BHD receiver, the circuits and amplifier noise, the internal filter response time delay, as well as the quantification errors of the A/D converter.

Indeed in the Q field our measurements are very close to the zero-point fluctuations and in the I field there is more additional noise, especially at higher N_S. For a pair of phase ϕ and amplitude A the standard deviation evaluates specifically with the phase parameter ϕ. Note that the detected signal is $Output(A,\phi)' = A\cos(\phi)$, and at π/2 and –π/2, the derivative of $|\cos(\phi)|$ is 0, while at phase 0 and π the derivative of $|\cos(\phi)|$ is 1, which makes the receiver more sensitive to phase fluctuation. As a matter of fact, the attenuation of optical signal power smoothes out the excess noise as compared to the vacuum fluctuation and the results appear to be closer to the quantum measurements.

In WCS communications, the additional power penalty in the simultaneous I-Q measurements increases the BER. Since the I-Q measurements are only necessary for the LO synchronization stage, the sequential I-Q measurements configuration using a digital synthetic Costas loop can operate at very low photon numbers and track the system phase drifts without the need of a pilot carrier modulation. Due to the technical limitations of the present experimental prototype, there is still a considerable margin of improvement, such as pulsed laser source with better spectral line-width, PIN photodiodes with faster response time, and RF amplifier with lower noise factor. Furthermore, the slow polarization drift can add additional impairments since the digital Costas loop adjusts the parameters of the low-pass filter according to power levels of the BPSK signal and the LO. In conclusion, thanks to its simple and flexible configuration, this technique can be used in diverse coherent optical applications for WCS signal detection. Although this scheme reduces half of the signal bit rate to beat with the LO in the I and the Q fields sequentially, high bit rate is attainable since the phase correction does not need heavy recursive algorithm for signal processing.

9.4 EXPERIMENTAL CHARACTERIZATION OF SQUEEZED COHERENT STATES

Experimental shot-noise reduction from squeezed light has been demonstrated in table-top interferometers [31-33], and it has been found and proven in different ways [34-36] that the quantum correlated light, e.g. can reduce quantum noise below the standard quantum limit (SQL). Harms *et al.* [37] have pointed out that signal-recycled interferometers can benefit from squeezed light similarly to conventional interferometers.

In this section we present a method for the phase-dependent squeezed level characterization of light using Mach-Zehnder based system as we have mentioned before. We synchronize the receiver using training frame, and reconstruct the "amplitude-phase" Wigner function by using inverse Radon function and standard back-projection algorithm.

9.4.1 QUADRATURE MEASUREMENTS OF 128 EQUIDISTANT PHASE STATES

In our experiments we successfully applied 128 equally spaced phase states modulation from 0 to 2π, i.e. $\phi_i = 2i\pi/128$, with $i = 0,1,2,...,127$, and the measurements are conducted according to the phase mismatch between the signal and the strong LO. For each phase state with mean photon number N_S, we make 12288 measurements. The photon numbers are calculated based on the measured vacuum state fluctuation as half photon energy. We adjust carefully the receiver as to allow an imbalance rate lower than 0.5% between the two input ports.

We apply a "ramp" signal from the function generator as to cover the different phase states from 0 to 360 degrees, at a repetition frequency of 250 kHz. The homodyne detector turns the laser beams into electric currant, and we sample the signal output of the balanced receiver by the PCI A/D converter, at a frequency of 32 MHz. Consequently the received data are stored into 128 files from which we measure the mean value and the standard deviation for each phase state.

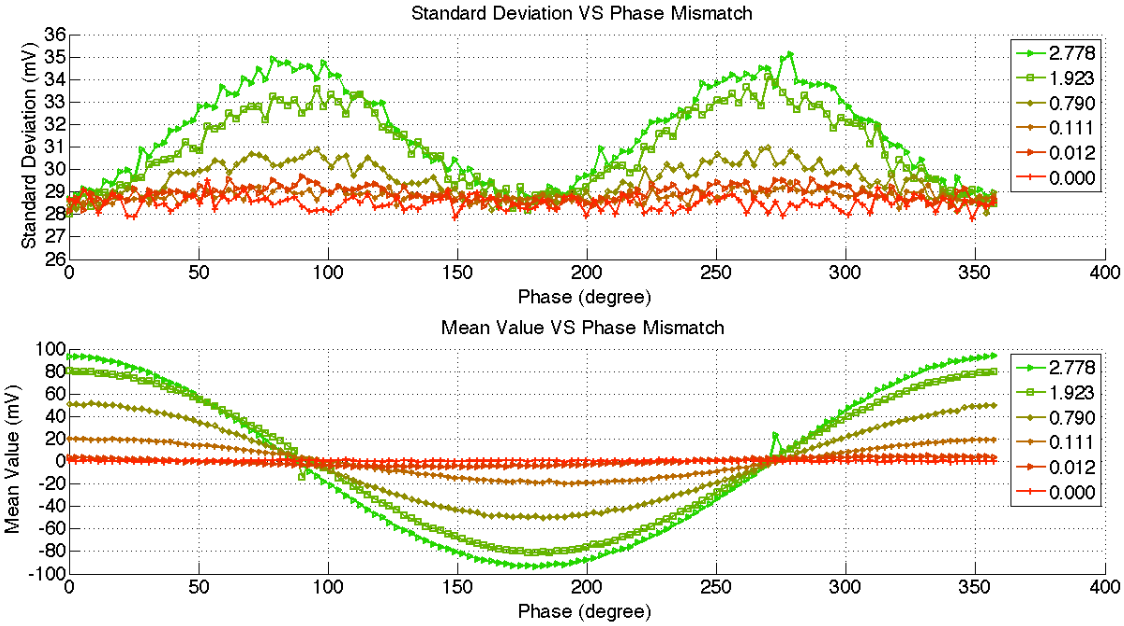


Figure 9.6 Measured amplitude standard deviation and mean value.

As shown in Figure 9.6, we have measured with six different mean photon number signals (as indicated by the inset legend), and we have observed that the standard deviations of the measurements reach at their minimum values at phase π/2 and –π/2, and at their maximum value at phase 0 and π. The measurements with $N_S = 0$ correspond to the vacuum state. It appears in our calculation that the measured standard deviation of the amplitude quadrature is phase-dependent, just as we have mentioned in section 9.3.

9.4.2 Wigner Function Reconstruction

In order to reconstruct the Wigner function, we build up a set of histograms for each phase state, from which we use the back projection algorithm to reconstruct the probability densities at different quadrature angles, as first mentioned in [38,39]. The transformation used is the inverse Radon-Transform in Matlab. For the signal processing, we select to use a linear transform without using any filter that could distort the original Wigner function.

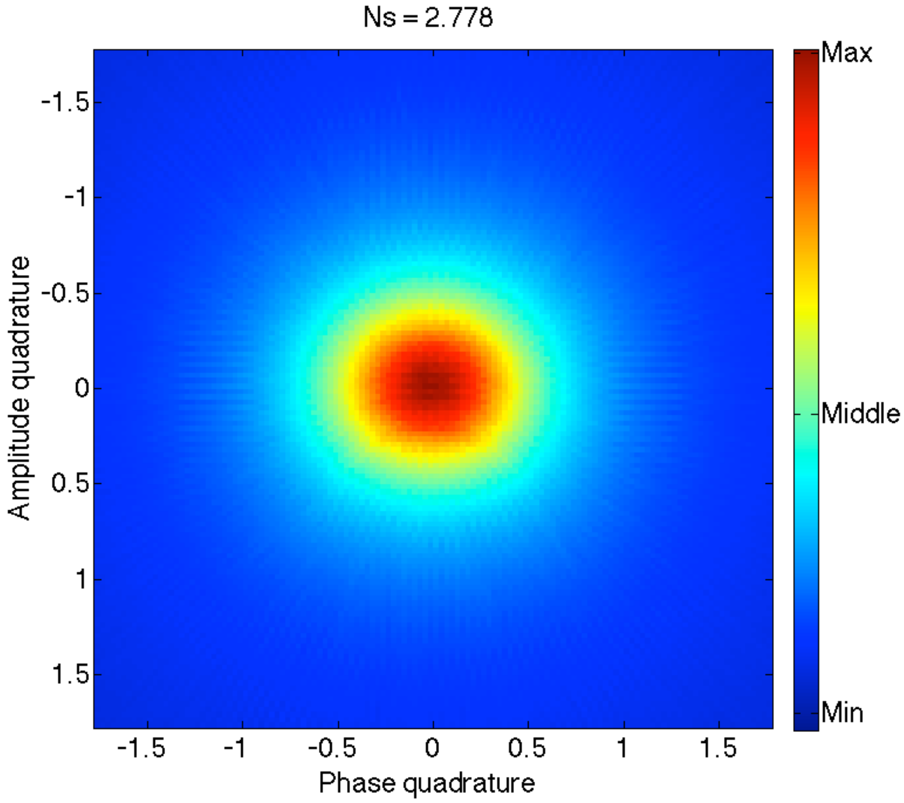


Figure 9.7 Reconstructed Wigner function for $N_S = 2.78$

For the Wigner function reconstruction altogether 12288×128=1572864 quadrature values have been measured, upon the 128 equidistant quadrature phase states. We have measured 6 Wigner functions at various signal power, defined by the mean photon number N_S. All these measurements are performed with very good phase modulation precision, i.e., phase drift are controlled less than 1°. As well the receiver has been well stabilized thanks to the phase error feedback loop using 50% received symbols as "training bits" so as to guarantee the reliable measurements especially for very low N_S.

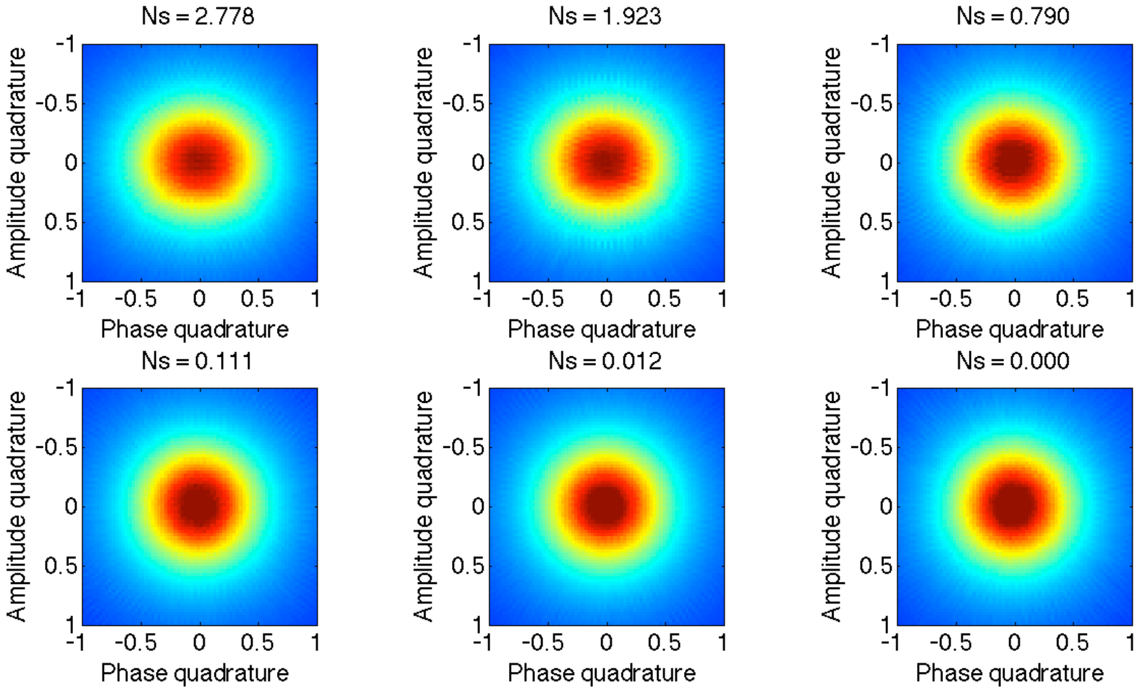


Figure 9.8 Reconstructed Wigner function for 6 signal photon numbers

In Figure 9.8, the Wigner functions reveal increasingly squeezing-ellipses with higher N_S, i.e. slightly squeezed amplitude quadrature and extended phase quadrature, as compared to the Wigner function of the vacuum states where $N_S = 0$. Therefore the lightwave does not operate as absolute coherent states, since the phase quadrature fluctuation $\Delta\phi$ is observed slightly greater than the amplitude quadrature fluctuation ΔA.

Nevertheless, the light source Avanex ILM module that we have measured demonstrates insignificant squeezing-ellipses, especially for weak signal level. In quantum cryptography applications where only $N_S < 1$ is required, we can approximately consider it as a source of coherent states. Due to the limited timeline and the inadequate laser sources, the system and security analysis of using the squeezed coherent states in the phase-modulation quantum key distribution have not been performed, however these aspects can also be very high research interests, just as the Heisenberg uncertainty itself.

REFERENCES

1. , L. G. Kazovsky, "Optical heterodyning versus optical homodyning: a comparison", *Journal of Optical Communications* **6,** 18-24 (1985).
2. T. Okoshi, "Recent advances in coherent optical fiber communication systems", *Journal of Lightwave Technology* **5,** 44-52 (1987).
3. A. H. Gnauck, and P. J. Winzer, "Optical phase-shift-keyed transmission", *Journal of Lightwave Technology* **23,** 115-130 (2005).
4. L. G. Kazovsky, G. Kalogerakis, and W.-T. Shaw, "Homodyne phase-shift-keying systems: past challenges and future opportunities", *Journal of Lightwave Technology* **24,** 4876-4884 (2006).
5. H. P. Yuen, and V. W. S. Chan, "Noise in homodyne and heterodyne detection", *Optics Letters* **8,** 177-179 (1983).
6. K.-P. Ho, *Phase-modulated optical communication systems* Ch. 4, (Springer 1st edition, 2005).
7. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, P. Grangier, "Quantum key distribution using gaussian-modulated coherent states", *Nature* **421,** 238-241 (2003).
8. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, R. Namiki, "Quantum cryptography using pulsed homodyne detection", *Physical Review A* **68,** 042331 (2003).
9. V. W. S. Chan, "Free-space optical communications", *Journal of Lightwave Technology* **24,** 4750-4762 (2006).

10. G. M. D’Ariano, M. G. A. Paris, M. F. Sacchi, “Quantum tomography”, *Advance in Imaging & Electron Physics* **128,** 205-308 (2003).

11. R. J. Glauber, “Coherent and incoherent states of the radiation field”, *Physical Review* **131,** 2766-2788 (1963).

12. C. W. Helstrom, *Quantum detection and estimation theory, Mathematics in Science and Engineering* **123,** (Academic Press, New York, 1976).

13. J. H. Shapiro, S. R. Shepard, N. C. Wong, “Ultimate quantum limits on phase measurement”, *Physical Review Letters* **62,** 2377-2380 (1989).

14. G. M. D’Arianno, M. G. A. Paris, R. Seno, “Homodyne detection of the phase through independent measurements”, 301-306, in *Quantum Interferometry*, De Martini, F., Denardo, G., Shih, Y., (Edition Weinheim, New York, 1996).

15. H. P. Yuen, R. S. Kennedy, M. Lax, “On optimal quantum receivers for digital signal detection”, *Proceeding IEEE* **58,** 1170-1173 (1970).

16. J. H. Shapiro, “On the near-optimum binary coherent-state receiver”, *IEEE Transaction of Information Theory* **26,** 490-491 (1980).

17. J. M. Geremia, “Distinguishing between coherent states with imperfect detection”, *Physical Review A* **70,** 062303 (2004).

18. G. P. Agrawal, *Fiber-optic Communication Systems* Ch. 10, (3rd edition, Wiley-Interscience, 2002).

19. H. P. Yuen, J. H. Shapiro, “Optical communication with 2-photon coherent states. Part III Quantum measurements realizable with photo-emissive detectors”, *IEEE Transaction of Information Theory* **6,** 78-82 (1980).

20. R. L. Cook, P. J. Martin, J. M. Geremia, "Optical coherent state discrimination using a real-time closed-loop quantum measurement", *Nature* **446,** 774-777 (2007).

21. H. L. Van Trees, *Detection, Estimation, and Modulation Theory*, (Wiley-Interscience, Publication 1968).

22. H. M. Wiseman, R. B. Killip, "Adaptive single-shot phase measurements: The full quantum theory", *Physical Review A* **57,** 2169-2185 (1998).

23. A. S. Holevo, "Optimal receiver of a binary coherent signal based on the principle of optical feedback", *Laser Physics* **13,** 1558-1561 (2003).

24. J. M. Fabrega, J. Prat, "Homodyne receiver prototype with time-switching phase diversity and feedforward analog processing", *Optics Letters* **32,** 463-465 (2007).

25. I. B. Djordjevic, "Optical homodyne PSK receivers with a Costas loop for long-haul communications", *Journal of Optical Communications* **23,** 154-158 (2002).

26. M. Seimetz, C. M. Weisert, "Options, feasability and availability of 2x4 90° hybrids for coherent optical systems", *Journal of Lightwave Technology* **24,** 1317-1322 (2006).

27. I. B. Djordjevic, M. C. Stefanovic, S. S. Ilic, G. T. Djordjevic, "An example of a hybrid system: coherent optical system with Costas loop in receiver-system for transmission in baseband", *Journal of Lightwave Technology* **16,** 177-183 (1998).

28. L. M. I. Habbab, J. M. Kahn, J. I. Greenstein, "Phase insensitive zero I.F. coherent optical system using phase switching", *Electronics Letters* **24,** 974--976 (1988).

29. Q. Xu, M. B. Costa e Silva, A. Arvizu, P. Gallion, and F. J. Mendieta - "Weak coherent state homodyne detection with sequential I-Q measurements", *Conference*

on Lasers and Electro-optics, Quantum Electronics and Laser Science Conference, CLEO/QELS and PhAST **JTuA114** (May 2008), San Jose, California, USA.

30. Q. Xu, A. Arvizu, P. Gallion, and F. J. Mendieta, "Homodyne in-phase and quadrature detection of weak coherent states with carrier phase tracking", submitted to *Journal of selected topics in Quantum Electronics*.
31. M. Xiao, L.-A. Wu and H. J. Kimble, "Precision measurement beyond the shot-noise limit", *Physical Review Letters* **59**, 278-281 (1987).
32. P. Grangier, R. E. Slusher, B. Yurke and A. LaPorta, "Squeezed-light–enhanced polarization interferometer", *Physical Review Letters* **59**, 2153--2156 (1987).
33. F. Jérémie, J. L. Vey, and P. Gallion, "Optical corpuscular theory of semiconductor laser intensity noise and intensity squeezed-light generation", *Journal of Optical Society of American B* **14**, 250--257 (1997).
34. W. G. Unruh, *Quantum Optics, Experimental Gravitation, and Measurement Theory*, 647, edited by P. Meystre and M. O. Scully (Plenum, New York, 1982).
35. J. Gea-Banacloche and G. Leuchs, "Squeezed states for interferometric gravitational-wave detectors", *Journal of Modern Optics* **34**, 793--811 (1986).
36. A. F. Pace, M. J. Collett and D. F. Walls, "Quantum limits in interferometric detection of gravitational radiation", *Physical Review A* **47**, 3173--3189 (1993).
37. J. Harms, Y. Chen, S. Chelkowski, A. Franzen, H. Vahlbruch, K. Danzmann, and R. Schnabel, "Squeezed-input, optical-spring, signal-recycled gravitational-wave detectors", *Physical Review D* **68**, 042001 (2003).

38. M. Beck, D. T. Smithey, J. Cooper, and M. G. Raymer, “Experimental determination of number - phase uncertainty relations”, *Optical Letters* **18**, 1259-1261 (1993).

39. S. Chelkowski, H. Vahlbruch, B. Hage, A. Franzen, N. Lastzka, K. Danzmann, and R. Schnabel, “Experimental characterization of frequency-dependent squeezed light”, *Physical Review A* **71**, 013806 (2005).

CONCLUSION

In our research at ENST ParisTech, we have studied and analyzed the interdisciplinary aspects of a quantum cryptography system towards a practical optical fiber QKD system implementation. Preliminary system tests have been validated using a Mach-Zehnder interferometer based QPSK modulation scheme.

We have chosen to integrate a QKD link by applying a signal–reference time-multiplexing scheme to minimize the system impairments. We have implemented an all fiber one-way QPSK quantum key distribution system at 1550nm using both photon counting and BHD configurations. An automatic optoelectronic feedback loop is implemented for the interferometric phase drift compensation.

We have developed a dual-threshold decision scheme for the BHD signal post-detection, and compared experimentally the performance of photon counting and BHD in terms of detection efficiency ρ and BER (or QBER). We point out that BHD is potentially more effective in terms of quantum key generation rate and system flexibility.

We have also investigated the security issues of the BHD QKD system under two main individual attacks: intercept-resend attack and intermediate-base attacks. A mixed attack strategy of signal power modification has also been analyzed. We have also measured the post-detection efficiency ρ, post-detection error rate BER_p, and conducted the security analysis under divers attacks for different threshold parameters X at 0 km, 25 km, 50 km, and 64 km. The trade-off is between the system security tolerance and the key generation rate: use a higher threshold when the transmission distance is longer or when the WCP is weaker. Accordingly, we have proposed the strategies to detect Eve's attacks by BER_p evaluations.

Alongside the development of our QKD system, we have also investigated into the weak coherent states homodyne communications with the researchers from CICESE in Mexico. The system setup is based on an interferometric self–homodyne configuration, which substantially relaxes the speed in the signal processor block, since the strong cross-correlation between the signal and the local oscillator fields yields a very narrowband post-detection process at baseband. Furthermore, the present advances in processor speed will surely allow the implementation of this kind of receivers for uncorrelated fields, providing additional capabilities for the mitigation of the optical channel impairments.

PERSPECTIVES

The information security systems of the 21st century require significant improvements due to the hardware and software advancements that meanwhile enhance the intruder's capacity. Quantum cryptography, as the only physically unbreakable security system, though still on its nascent phase, will see its full utility and integration to the current telecom infrastructure in the coming future.

The possible future directions of the research at ENST ParisTech can be extended as the followings.

- Continuing the security analysis of the photon counting and the dual-threshold balanced homodyne detection schemes. A comprehensive analysis of the most appropriate signal pulse power, always less than 1 photon/bit, is to be found for a given transmission distance, under the maximum acceptable post detection BER. Especially for the BHD scheme, since the post detection BER and the detection efficiency are directly related to the threshold parameter value and the transmission distance.

- Decoy states protocol or other eavesdropper-detection protocols can be integrated to the BHD scheme to enhance the system security. Such a multi-state protocol could possibly sacrifice the efficient key generation rate to make the system more robust to the potential attacks, i.e. the mixed or joint attacks.

- We are also envisaging the lateral integration of the physical layer with the application layer that has been developed in the department of INFRES in ENST. Under the French government funding for the research project ANR high bit-rate and versatile quantum-secured networks (HQNET), a system demonstration platform is to be developed on collaboration with SMART Quantum and the Femto group in the Université de Franche-Comté.

- Besides, the studies of the quantum nature of the light and the experimental characterization of the laser source using Wigner function reconstruction algorithm can be extended from what we have described on chapter 9.4.2.

PUBLICATIONS

JOURNAL PUBLICATIONS

1. **Q. XU**, A. ARVIZU, P. GALLION, and F. J. MENDIETA - “Homodyne In-Phase and Quadrature Detection of Weak Coherent States with Carrier Phase Tracking”, to be published in *Journal of selected topics in Quantum Electronics*, November 2009.
2. **Q. XU**, M. SABBAN, and P. GALLION - “Homodyne Detection of Weak Coherent Optical Pulse with Selection on Decision Opportunity- Applications to Quantum Cryptography”, Vol. 51, Issue 8, 1934-1939, *Microwave and Optical Technology Letters*, 13 May 2009.
3. **Q. XU**, M. SABBAN, M.B. COSTA e SILVA, P. GALLION, and F.J. MENDIETA - “Dual-Threshold Balanced Homodyne Detection in 1550 nm Optical Fiber Quantum Cryptography System”, Vol. 27, No. 12, *IEEE Journal of Lightwave Technology*, 2009.
4. M.B. COSTA e SILVA, **Q. XU**, S. AGNOLINI, P. GALLION, and F.J. MENDIETA - “Homodyne Detection for Quantum Key Distribution: an Alternative to Photon Counting in BB84 protocol”, *Proceedings of SPIE -Volume 6343*: Photonics North 2006, Pierre Mathieu, Editor, SPIE Bellingham, WA, September 2006.

INTERNATIONAL CONFERENCE PUBLICATIONS

5. **Q. XU**, M. SABBAN, P. GALLION, and F.J. MENDIETA - "Quantum Key Distribution System using Dual-threshold Homodyne Detection*", 6th IEEE International Conference on Information and Communication Technologies RIVF 2008*, Ho Chi Minh City (Vietnam), July 13-17, 2008.
6. **Q. XU**, M. SABBAN, P. GALLION, and F.J. MENDIETA - "Dual-threshold Receiver for 1550nm Homodyne QPSK Quantum Key Distribution System", *Coherent Optical Technologies and Applications (COTA) Topical Meeting of the OSA*, Paper CWC4, Boston (Massachusetts, USA), July 13-16, 2008.
7. M. SABBAN, **Q. XU**, P. GALLION, and F.J.MENDIETA - "Security Evaluation of Dual-Threshold Homodyne Quantum Cryptographic Systems", *2008 Quantum Entanglement and Decoherence: 3rd International Conference on Quantum Information (ICQI) Topical Meeting. ICQI*, Paper JMB77, Boston (Massachusetts, USA), July 13-16, 2008.
8. **Q. XU**, M.B. COSTA e SILVA, A. ARVIZU, P. GALLION, and F.J. MENDIETA - "Weak Coherent State Homodyne Detection with Sequential I-Q Measurements", *Conference on Lasers and Electro-optics, Quantum Electronics and Laser Science Conference, CLEO/QELS and PhAST 2008*, Paper JTuA114, San Jose (California, USA), May 2008.
9. **Q. XU**, M.B. COSTA e SILVA, P. GALLION, and F.J. MENDIETA - "Auto-Compensating Quantum Cryptosystem Using Homodyne Detection", *Conference on*

optical fiber communication OFC'2008, Paper JWA49, San Diego (California, USA), February 2008.

10. **Q. XU**, M. B. COSTA e SILVA, P. GALLION, and F. J. MENDIETA - "Experimental Super Homodyne Quantum Key Distribution System", *Summer School e-Photon/One+ 2007*, Brest (France), July 2007.
11. **Q. XU**, M.B. COSTA e SILVA, P. GALLION, and F.J. MENDIETA - "One Way Differential QPSK Quantum Key with Channel Impairment Compensation", *Conference on Lasers and Electro-optics CLEO Europe, JOINT CLEO/Europe-IQEC 2007 SYMPOSIA*, Paper JSI 3, München (Germany), June 2007.
12. **Q. XU**, M.B. COSTA e SILVA, S. GUILLEY, J-L. DANGER, P. BELLOT, P. GALLION, and F. J. MENDIETA , "Towards Quantum Key Distribution System using Homodyne Detection with Differential Time-Multiplexed Reference", *5th IEEE International Conference on Information and Communication Technologies RIVF 2007*, Hanoi (Vietnam), March 2007.
13. **Q. XU**, M.B. COSTA e SILVA, S. AGNOLINI, P. GALLION, and F.J. MENDIETA - "Photon Counting and Super Homodyne Detection of Weak QPSK Signals for Quantum Key Distribution Applications", *EOS Annual Meeting 2006, Topical Meeting on Extreme Optics (QEOD/EPS and EOS)*, TOM2 Page 110-111, Paris (France), October 2006.
14. M.B. COSTA e SILVA, **Q. XU**, S. AGNOLINI, S. GUILLEY, J-L. DANGER, P. GALLION, and F. J. MENDIETA - "Integrating a QPSK Quantum Key Distribution Link", *European Conference on Optical Communication ECOC 2006, CLEO Focus*

Meeting on Nonlinear, Quantum and Chaotic Optics: New Directions in Photonics and Optical Communications, Paper Tu4.1.2, Cannes (France), September 2006.

15. M.B. COSTA e SILVA, **Q. XU**, S. AGNOLINI, P. GALLION, and F.J. MENDIETA - “Homodyne QPSK Detection for Quantum Key Distribution”, *Coherent Optical Technologies and Applications (COTA) Topical Meeting of the OSA*, Paper CFA2, Whistler (British Columbia, Canada), June 2006.
16. M.B. COSTA e SILVA, **Q. XU**, S. AGNOLINI, P. GALLION, and F.J. MENDIETA - “Homodyne Detection for Quantum Key Distribution: an Alternative to Photon Counting”, International Conference On Applications of Photonic Technology, *Photonics North 2006*, Quebec City (Canada), June 2006.

APPENDIX A: BRA AND KET VECTORS

"Bra" and "ket" spaces are two equivalent vector spaces that describe the same state space. A ket vector is $|a\rangle = \begin{pmatrix} a_x \\ a_y \end{pmatrix}$, a bra vector $\langle a| = \begin{pmatrix} a_x^{\ *} & a_y^{\ *} \end{pmatrix}$. For every ket vector $|a\rangle$, bra vector is the adjoint vector, or complex conjugate transpose, of the corresponding ket vector. For complex-valued bra-ket vectors, the inner product is used to find length of a vector and is determined by multiplying its bra representation $\langle a|$ with its ket representation $|a\rangle$: $\|a\|^2 = \langle a|a\rangle$, where $\|\cdot\|$ is the norm of the vector.

APPENDIX B: POLARIZATION MISMATCH IN HOMODYNE DETECTION

Let's first see a classical description of polarization. Consider a time-harmonic monochromatic plane wave that travels in the $\hat{z}$ direction ($k \bullet r = kz$), since $k \bullet E = 0$ in vacuum, so there is no $\hat{z}$ component to the electric field. Thus without loss of generality, the form of electric field vector is

$$E(z,t) = \begin{pmatrix} E_x e^{j\phi_x} \\ E_y e^{j\phi_y} \end{pmatrix} e^{j(\omega t - kz)} \tag{B.1}$$

In an elliptical equation, the field amplitudes as projected along the $\hat{x}$ and $\hat{y}$ direction are

$$\begin{cases} x = E_x \cos(\omega t) \\ y = E_y \cos(\omega t + \phi) \end{cases} \tag{B.2}$$

where $\phi = \phi_y - \phi_x$ and $\frac{x^2}{E_x^{\ 2}} + \frac{y^2}{E_y^{\ 2}} - \frac{2xy}{E_x E_y}\cos\phi = \sin^2\phi$. And there are three independent variables that govern the shape of the ellipse: E_x, $E_y$and ϕ.

If we define $\tan\chi = E_y / E_x$ and $E_0 = \sqrt{E_x^{\ 2} + E_y^{\ 2}} e^{j\phi_x} e^{j(\omega t - kz)}$, then the Jones vector of the wave field can be rewritten in the normalized form:

$$E = E_O \begin{pmatrix} \cos\chi \\ \sin\chi \cdot e^{j\phi} \end{pmatrix} \tag{B.3}$$

In the coherent homodyne detection, the signal wave and reference wave mix after the Mach-Zehnder interferometer. We represent the signal field by

$$E_{signal} = E_S e^{j\theta} \begin{pmatrix} \cos\chi_1 \\ \sin\chi_1 \cdot e^{j\phi_1} \end{pmatrix} \tag{B.4}$$

and the reference field by

$$E_{reference} = E_L \begin{pmatrix} \cos\chi_2 \\ \sin\chi_2 \cdot e^{j\phi_2} \end{pmatrix} \tag{B.5}$$

thus the length property of $E_{signal} + E_{reference}$ is

$$\begin{aligned} &\left\| E_{signal} + E_{reference} \right\| \\ &= E_{signal} E_{reference}{}^{*} + E_{signal}{}^{*} E_{reference} \\ &= E_S{}^2 + E_L{}^2 + E_S E_L \cos\chi_1 \cos\chi_2 \cdot 2\cos\theta + E_S E_L \sin\chi_1 \sin\chi_2 \cdot 2\cos(\phi_1 - \phi_2 + \theta) \end{aligned} \tag{B.6}$$

If we assume $\chi_1 = \chi_2 + \Delta\chi$, i.e. $\Delta\chi = \chi_1 - \chi_2$, and we obtain:

$$\begin{aligned} &\left\| E_{signal} + E_{reference} \right\| \\ &= E_S{}^2 + E_L{}^2 + E_S E_L \cos(\Delta\chi) \cdot 2\cos\theta + E_S E_L \sin\chi_1 \sin\chi_2 \cdot \left[\left(\cos(\Delta\phi) - 1 \right) - \sin\Delta\phi \sin\theta \right] \end{aligned} \tag{B.7}$$

In an ideal case, E_{signal} and $E_{reference}$ have the same polarization i.e. $\phi_1 = \phi_2$, $\chi_1 = \chi_2$, we can obtain:

$$\left\| E_{signal} + E_{reference} \right\| = E_S{}^2 + E_L{}^2 + E_S E_L \cdot 2\cos\theta \tag{B.8}$$

The output of Detector 2 is $E_{signal} - E_{reference}$, the length property can be obtained:

$$\left\| E_{signal} - E_{reference} \right\| = E_S{}^2 + E_L{}^2 - E_S E_L \cdot 2\cos\theta \tag{B.9}$$

Therefore when $\Delta\phi = 0$, we can obtain the balanced output:

$$\left\| E_{signal} + E_{reference} \right\| - \left\| E_{signal} - E_{reference} \right\| = E_S E_L \cdot 4\cos\theta \tag{B.8}$$

APPENDIX C: BB84 PROTOCOL USING DUAL-THRESHOLD BALANCED HOMODYNE

C.1 PROTOCOL

Alice randomly chooses one of the four coherent states $\{|\alpha\rangle,|i\alpha\rangle,|-\alpha\rangle,|-i\alpha\rangle\}$ with $\alpha > 0$. Then Bob randomly measures one of the two quadratures $\{\hat{x}_1,\hat{x}_2\}$, in which x_1, x_2 do not commute with each other and $[\hat{x}_1,\hat{x}_2] = \frac{i}{2}$. If Alice uses a pulsed light source, the coherent state is the eigenstate of the annihilation operator $\hat{a} = x_1 + ix_2$ of the pulse mode. We say a measure is of base coincidence when Bob measures $\hat{x}_1$ when Alice sends $|\pm\alpha\rangle$ or measures with $\hat{x}_2$ when Alice sends $|\pm i\alpha\rangle$ (correct base). Otherwise we say a measure of base anti-coincidence (wrong base).

For the pulse of base coincidence Bob sets the threshold X ($X \geq 0$) and constructs his bit sequence by the following decision:

$$bit\ value = \begin{cases} 1 & if(x > X) \\ 0 & if(x < -X) \\ inconclusive & otherwise \end{cases} \tag{C.1}$$

where x is the result of Bob's measurement

Alice's bit values are determined by the different symbols: Alice regards $\{|\alpha\rangle,|i\alpha\rangle\}$ as bit "1" and $\{|-\alpha\rangle,|-i\alpha\rangle\}$ as bit "0". Also the density operator of the signal sent by Alice is described by:

$$\hat{\rho} = \frac{1}{4}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha| + |i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right) \tag{C.2}$$

Here the factor $1/4$ assumes that each of the four states appears with equal probability. Bob or Eve's work is to distinguish the four states. Since the four states are not orthogonal with each other, complete differentiation is impossible. After Alice announces the base choice, i.e., the quadrature on which she encoded the bit information, then the density operator is reduced to

$$\hat{\rho}_1 = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right) \tag{C.4}$$

$$\text{or } \hat{\rho}_2 = \frac{1}{2}\left(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right) \tag{C.5}$$

for the announced quadrature $\hat{x}_1$ and $\hat{x}_2$, respectively.

C.2 QUADRATURE MEASUREMENTS

We introduce the probability density that the outcome x_ϕ is obtained by measuring $\hat{x}_\phi = \hat{x}_1 \cos\phi + \hat{x}_2 \sin\phi$ of a coherent state $|\alpha\rangle$:

$$\left|\langle x_\phi|\alpha\rangle\right|^2 = \sqrt{\frac{2}{\pi}}\exp\left(-2\left(x_\phi - \alpha\cos\phi\right)^2\right) \tag{C.6}$$

Then the probability distribution of quadrature measured by Bob is written as:

$$\langle x_i|\hat{\rho}_j|x_i\rangle = \begin{cases} \sqrt{\dfrac{1}{2\pi}}\left(\exp\left(-2\left(x_i - \alpha\right)^2\right) + \exp\left(-2\left(x_i + \alpha\right)^2\right)\right) & \text{if } i = j \\ \sqrt{\dfrac{2}{\pi}}\exp\left(-2x_i^{\,2}\right) & \text{if } i \neq j \end{cases} \tag{C.7}$$

with $i,j = 1,2$ (see Fig. 1). Here $i = j$ stands for base coincidence pulses and $i \neq j$ is for base anticoincidence ones. When Alice announces the states (both base and bit value) she sent, Bob observes the quadrature distributions for the coherent states. The quadrature distributions represent the conditional probability that characterizes the signal detection and thus any detectable disturbance should appear on the statistic distributions.

C.3 SINGLE THRESHOLD BIT ERROR RATE

In classical coherent detection, the threshold is $X = 0$. As the bit values “0” and “1” appear with the same probability, to calculate the bit error rate (BER) we can consider the bit value as “1”. With the average photon number per signal pulse $\alpha = N_S$ we can obtain bit error rate:

$$\begin{aligned} BER &= \int_{-\infty}^{0} \left|\left\langle x_\phi \middle| \alpha \right\rangle\right|^2 dx \\ &= \sqrt{\frac{2}{\pi}} \int_{-\infty}^{0} \exp\left(-2(x_1 - \alpha)^2\right) dx_1 \\ &= 1/2\, erfc\left(\sqrt{2N_S}\right) \end{aligned} \tag{C.8}$$

C.4 DUAL THRESHOLD POST-DETECTION EFFICIENCY

With the normalized threshold X, the post-detection efficienc ρ, which is defined as the probability of a conclusive judgment:

$$\begin{aligned} \rho(X, N_S) &= \sqrt{\frac{2}{\pi}} \int_{-\infty}^{-X} \exp\left(-2(x_1 - \alpha)^2\right) dx_1 + \sqrt{\frac{2}{\pi}} \int_{X}^{\infty} \exp\left(-2(x_1 - \alpha)^2\right) dx_1 \\ &= 1/2\, erfc\left[(2N_S)^{1/2}(X+1)\right] + 1/2\, erfc\left[(2N_S)^{1/2}(X-1)\right] \end{aligned} \tag{C.9}$$

C.5 DUAL THRESHOLD BIT ERROR RATE

The post-detection BER is defined as the erroneous bit rate in the retained bit, therefore those bit values between $(-X, X)$ are discarded.

$$\begin{aligned} BER_p &= 1/\rho(X, N_S) \cdot \sqrt{\frac{2}{\pi}} \int_{-\infty}^{-X} \exp\left(-2(x_1 - \alpha)^2\right) dx_1 \\ &= \left(1/2\rho(X, N_S)\right) \cdot erfc\left[(2N_S)^{1/2}(X+1)\right] \end{aligned} \tag{C.10}$$

C.6 EVE'S INTERCEPT RESEND ATTACK

In this attack, Eve splits the intercepted signal into two parts She splits the signal into two pulses of half intensity by using a 50:50 beam splitter (BS) and measures the quadrature $\hat{x}_1$ of one pulse and the quadrature $\hat{x}_2$of the other pulse, as on the two bases; accordingly she obtains a pair measured values x_1 and x_2.

Eve then record the symbol value by choosing a more probable value:

$$signal_{Eve} = \begin{cases} |\alpha\rangle & if\left(x_1 > |x_2|\right) \\ |i\alpha\rangle & if\left(x_2 > |x_1|\right) \\ |-\alpha\rangle & if\left(-x_1 > |x_2|\right) \\ |-i\alpha\rangle & if\left(-x_2 > |x_1|\right) \end{cases} \tag{C.11}$$

Without loss of generality, we consider the case that Alice sent $|\alpha\rangle$. The probability that Eve gets an outcome $\left(x_1,x_2\right)$ is given by the product of the two quadrature distributions for the split coherent states. We can thus have the probability density function:

$$\begin{aligned} Q_n\left(x_1,x_2\right) &= \left|\left\langle x_1 \middle| \frac{\alpha}{\sqrt{2}} \right\rangle\right|^2 \left|\left\langle x_2 \middle| \frac{\alpha}{\sqrt{2}} \right\rangle\right|^2 \\ &= \frac{2}{\pi}\exp\left(-2\left(x_1 - \sqrt{\frac{N_S}{2}}\right)^2 - 2x_2{}^2\right) \end{aligned} \tag{C.12}$$

We define P_+ as the probability that Eve resends the correct bit state on the correct base:

$$\begin{aligned} \mathrm{P}_+ &= \iint_{x_1>|x_2|} Q_n\left(x_1,x_2\right)dx_1dx_2 \\ &= \iint_{x_1>|x_2|} \frac{2}{\pi}\exp\left(-2\left(x_1 - \sqrt{\frac{N_S}{2}}\right)^2 - 2x_2{}^2\right)dx_1dx_2 \end{aligned} \tag{C.13}$$

If we represent $\left(x_1,x_2\right)$ by $\left(u,v\right)$ with $u > 0, v > 0$

$$\begin{cases} x_1 = \frac{1}{\sqrt{2}}(u+v) \\ x_2 = \frac{1}{\sqrt{2}}(u-v) \end{cases} \tag{C.14}$$

The Jacobian matrix (the matrix of all first-order partial derivatives of a vector-valued function) is given by:

$$J = \begin{bmatrix} \frac{\partial x_1}{\partial u} & \frac{\partial x_1}{\partial v} \\ \frac{\partial x_2}{\partial u} & \frac{\partial x_2}{\partial v} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \tag{C.15}$$

And the Jacobian determinant is given by:

$$J = \begin{vmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{vmatrix} = 1 \tag{C.16}$$

Then we replace (x_1,x_2) by (u,v) in P_+, and we have:

$$\begin{aligned} \mathrm{P}_+ &= \iint_{u>0,v>0} \frac{2}{\pi} \exp\left(-2\left(\frac{1}{\sqrt{2}}(u+v) - \sqrt{\frac{N_S}{2}}\right)^2 - 2\left(\frac{1}{\sqrt{2}}(u-v)\right)^2\right) dudv \\ &= \iint_{u>0,v>0} \frac{2}{\pi} \exp\left(-2u^2 - 2v^2 - N_S + 2u\sqrt{N_S} + 2v\sqrt{N_S}\right) dudv \\ &= \iint_{u>0,v>0} \frac{2}{\pi} \exp\left(-2\left(u - \frac{\sqrt{N_S}}{2}\right)^2 - 2\left(v - \frac{\sqrt{N_S}}{2}\right)^2\right) dudv \\ &= \frac{2}{\pi}\left(\int_0^\infty \exp-2\left(u - \frac{\sqrt{N_S}}{2}\right)^2 du\right)^2 \\ &= \frac{1}{\pi}\left(\int_{\sqrt{\frac{N_S}{2}}}^\infty \exp\left(-u^2\right) du\right)^2 \\ &= \frac{1}{4}\left(erfc\left(-\sqrt{\frac{N_S}{2}}\right)\right)^2 \end{aligned} \tag{C.17}$$

Then we define P_ as the probability that Eve resends the wrong bit state on the correct base:

$$\begin{aligned}
\mathrm{P}_{-} &= \iint_{-x_1>|x_2|} Q_n\left(x_1,x_2\right)dx_1dx_2 \\
&= \iint_{-x_1>|x_2|} \frac{2}{\pi}\exp\left(-2\left(x_1-\sqrt{\frac{N_S}{2}}\right)^2-2x_2{}^2\right)dx_1dx_2 \\
&= \iint_{x_1>|x_2|} \frac{2}{\pi}\exp\left(-2\left(x_1+\sqrt{\frac{N_S}{2}}\right)^2-2x_2{}^2\right)dx_1dx_2 \\
&= \frac{1}{4}\left(erfc\left(\sqrt{\frac{N_S}{2}}\right)\right)^2
\end{aligned} \qquad \text{(C.18)}$$

and $\mathrm{P}_{\perp}$ as the probability that Eve resends the bit state on the wrong base:

$$\begin{aligned}
\mathrm{P}_{\perp} &= \iint_{|x_2|>|x_1|} Q_n\left(x_1,x_2\right)dx_1dx_2 \\
&= \iint_{|x_2|>|x_1|} \frac{2}{\pi}\exp\left(-2\left(x_1-\sqrt{\frac{N_S}{2}}\right)^2-2x_2{}^2\right)dx_1dx_2 \\
&= \frac{1}{4}\left(erfc\left(\sqrt{\frac{N_S}{2}}\right)\right)\left(erfc\left(-\sqrt{\frac{N_S}{2}}\right)\right)
\end{aligned} \qquad \text{(C.19)}$$

APPENDIX D: HEISENBERG UNCERTAINTY RELATION FOR COHERENT STATES

For Glauber's [1] coherent states, the probability density functions (PDF) of the outcomes of the independent measurements on the in-phase and quadrature components are both Gaussian functions with variance $\sigma^2 = 1/4$, hence the standard deviation $\sigma = 1/2$.

The PDF of the independent measurements X_I, X_Q of the in-phase component with average value α_I, or the quadrature component with average value α_Q of a coherent state is:

$$P\left(X_{I/Q}\right) = \sqrt{\frac{2}{\pi}} \exp\left[-2\left(X_{I/Q} - \alpha_{I/Q}\right)^2\right] \tag{D.1}$$

Furthermore the variances $\left\langle \Delta X_I{}^2 \right\rangle = \left\langle \left(\hat{X}_I - \left\langle \hat{X}_I \right\rangle\right)^2 \right\rangle$, $\left\langle \Delta X_Q{}^2 \right\rangle = \left\langle \left(\hat{X}_Q - \left\langle \hat{X}_Q \right\rangle\right)^2 \right\rangle$ on the two non-commutating observables are subject to the Heisenberg uncertainty relation:

$$\left\langle \Delta X_I{}^2 \right\rangle \left\langle \Delta X_Q{}^2 \right\rangle \geq \frac{1}{16} \tag{D.2}$$

A coherent state is a minimum uncertainty state in which the uncertainty $\Delta X_I = \frac{1}{2}$ and $\Delta X_Q = \frac{1}{2}$ is bounded by the zero-point fluctuation energy, so called the vacuum fluctuations.

REFERENCES

1. R. J. Glauber, "Coherent and incoherent states of the radiation field", *Physical Review* **131**, 2766-2788 (1963).