Interférences quantiques : études et applications

Stucki, Damien

UNIVERSITÉ DE GENÈVE FACULTÉ DES SCIENCES

Groupe de Physique Appliquée Professeur N. Gisin

Interférences quantiques :

études et applications

THÈSE

présentée à la Faculté des sciences de l'Université de Genève
pour obtenir le grade de Docteur ès sciences, mention physique

par

Damien Stucki

de Buchholterberg (Berne)

Thèse N° 3770

GENÈVE
2006

La Faculté des sciences, sur le préavis de Messieurs N. GISIN, professeur ordinaire et directeur de thèse (Groupe de physique appliquée), H. ZBINDEN, docteur (Groupe de physique appliquée), W. MUNRO, docteur (Hewlett-Packard Laboratories – Bristol, United Kingdom), et G. RIBORDY, docteur (id Quantique SA – Genève, Suisse), autorise l'impression de la présente thèse, sans exprimer d'opinion sur les propositions qui y sont énoncées.

Genève, le 20 juin 2006

Thèse - 3770 -

Le Doyen, Pierre SPIERER

Interférences quantiques : études et applications

Damien Stucki

Table des matières / Contents

Remerciements

Cette thèse en optique a été faite dans le groupe de physique appliquée, GAP-Optique, de l'université de Genève. Je remercie son directeur, le Professeur Nicolas Gisin, de m'avoir donné la possibilité de faire cette thèse.

Je vais aussi remercier l'ensemble des personnes passées ou toujours présentes au GAP-Optique. J'ai apprécié leur aide pour répondre à des questions expérimentales et théoriques. J'ai aussi apprécié la bonne ambiance durant le travail ou lors des diverses sorties que nous avons faites ensemble. Je remercie par ordre alphabétique : Alexios, André, Antonio, Barbara, Claudio, Cyril, Daniel C., Daniel S., Grégoire, Guilherme, Hugo, Hugues, Ivan, Jean-Daniel, Jeroen, Ketil, Laurent, Lilia, Mark, Matthäus, Matthias, Mikael, Nicolas B., Nicolas G., Olivier G., Olivier L., Philippe, Rob, Sara, Sébastien, Sofyan, Sylvain, Thomas, Valério, Wolfgang et ceux que j'aurais pu oublier.

Je vais encore remercier Rémy qui m'a appris les bases de la mécanique et les secrétaires Claudine, Chéryl, Denise, Isabel, Laurence et Nathalie qui m'ont permis de résoudre des problèmes administratifs.

Finalement, je vais remercier ma famille qui durant cette thèse, comme à son habitude, m'a activement soutenu.

Première partie

Version française

Chapitre 1

Introduction

Au cours du 19e siècle avec Young et Fresnel, puis par la suite avec Maxwell et sa théorie électromagnétique, une théorie moderne, ondulatoire permet de bien expliquer les phénomènes d'optique. Seuls le phénomène photoélectrique et la radiation du corps noir avec la catastrophe ultraviolette posaient encore quelques problèmes. En 1900, afin d'éliminer la catastrophe ultraviolette, Planck introduit l'idée que les radiations thermiques ne puissent être émises ou absorbées que sous forme de quanta discrets [1]. En 1905, parmi les quatre papiers révolutionnaires publiés par Einstein, l'un d'entre eux [2] pose véritablement les bases de la révolution de la mécanique quantique, la théorie qui décrit ce qu'il se passe au niveau des particules. Reprenant l'idée de Planck, Einstein explique que les corpuscules ou quanta de lumière ne découlent pas seulement d'astuces théoriques, mais que ces quanta représentent la lumière même. Il donne une explication complète de l'effet photoélectrique, ce qui lui vaudra le prix Nobel en 1921. En 1924, les quanta de lumière sont détectés directement pour la première fois par effet Compton (prix Nobel en 1927). En 1926, un chimiste, du nom de Lewis, introduit le nom « photon » pour qualifier les quanta de lumière.

Durant les années 1925-1927, grâce à Dirac, Schrödinger, Born et Heisenberg entre autres, la théorie de la mécanique quantique naît véritablement. Durant cette période, les fondements de la théorie quantique tels qu'ils sont encore présentés de nos jours sont posés. Un des résultats importants de cette période est qu'en mécanique quantique, le résultat d'une mesure est de type probabiliste. Ainsi généralement, si nous mesurons des systèmes quantiques préparés identiquement, nous aurons des résultats différents d'une mesure à une autre. De plus, Heisenberg publie un papier dans lequel, il énonce le principe d'incertitude ou principe d'indétermination [3]. Ce principe énonce qu'il n'est pas possible de connaître simultanément et avec une précision arbitrairement élevée certains couples de grandeurs physiques, par exemple, la position et l'impulsion d'une particule. Si nous partons d'un ensemble de particules préparées dans un état déterminé, en faisant une série de mesures de position ou d'impulsion, nous aurons alors un ensemble de résultats avec une certaine distribution. Cette distribution est pour une part due aux instruments de mesure. Cependant, selon le principe d'incertitude, même avec des instruments parfaits, il restera toujours une incertitude sur les mesures. Plus précisément, pour l'exemple considéré, le produit des écarts types de la position et de l'impulsion sera toujours supérieur à une certaine valeur. Dans le cas limite, où la mesure de la position serait parfaite, l'incertitude sur l'impulsion serait infinie. Il faut bien comprendre que cela n'est pas dû à des limitations expérimentales, aux instruments de mesure, mais cette limite est une limite fondamentale de la physique.

Une des conséquences du principe d'incertitude d'Heisenberg est l'impossibilité de connaître de manière parfaite un état quantique quelconque inconnu. Par exemple, l'impulsion et la position de la particule ne pourront pas être connues parfaitement. Ainsi, il ne sera pas possible d'en effectuer une copie parfaite. Ce comportement est très différent par rapport au monde classique de tous les jours, dans lequel il est possible de copier un objet. Les imperfections des copies classiques sont uniquement dues aux imperfections des instruments utilisés pour mesurer l'original et fabriquer les copies. Quantiquement, la précision des copies sera limitée par les fondements de la physique quantique. Cela va permettre l'émergence de la cryptographie quantique bien des années plus tard (chapitres 2 et 3).

L'interprétation probabiliste de la mécanique quantique ne plaisait pas à entre autres à Einstein, qui a dit « Dieu ne joue pas aux dés ». Pour expliquer cela, en 1935, Einstein, Podolsky et Rosen publient un célèbre papier [4] décrivant le paradoxe EPR, tel qu'il sera appelé par la suite : paradoxe décrivant les propriétés étonnantes de non-localité quantique. Ce papier voulait démontrer que la mécanique quantique était incomplète et ne décrit pas toute la réalité. Il explique qu'il est possible que des particules dans des états particuliers, états qui seront dits intriqués par la suite, présentent des corrélations lorsqu'ils présentent une séparation de type espace. Les états intriqués à deux particules sont définis par le fait que, jusqu'à ce que le processus de mesure intervienne, l'état de l'une ou l'autre des particules n'est pas défini, seul l'état global est défini. Par exemple, des photons intriqués en polarisation peuvent avoir simultanément les deux une polarisation verticale et les deux une polarisation horizontale. Séparons ces deux photons avec précaution. Tant que nous n'avons pas fait de mesure, les photons restent en superposition de polarisations horizontale et verticale. Mais lorsque nous mesurons un photon selon une polarisation, le second prend immédiatement la même. Pour Einstein *et al.*, cela paraissait inconcevable et donc la mécanique quantique devait être incomplète.

Le paradoxe EPR, qui était initialement une expérience de pensée, est par la suite devenu un vrai problème expérimental grâce aux inégalités de Bell [5]. Cette famille d'inégalité, dont la première fût proposée par John Bell, a permis d'envisager des expériences. Ces inégalités sont violées par la théorie quantique, mais pas par des théories classiques et locales. Freedman et Clauser [6], Fry et Thompson [7], puis Aspect, Dalibard et Roger [8] furent parmi les premiers à violer les inégalités de Bell. Ainsi, la non-localité des corrélations quantiques a été démontrée et donc Einstein *et al.* semblent avoir tort. Il faut toutefois noter que diverses échappatoires existent. Par exemple, il y a l'échappatoire de détection. Elle provient du fait que lorsque la probabilité de détection est inférieure à 100 %, alors, nous pourrions dire que la violation des inégalités de Bell n'est effective que pour le sous-ensemble des particules mesurées. Bien que différentes expériences aient permis de fermer l'une ou l'autre des échappatoires, aucune expérience n'a permis de toutes les fermer simultanément. Ces expériences vont ouvrir la porte à l'information quantique.

En effet, depuis le milieu des années 1980, ce nouveau champ de la mécanique quantique a émergé. L'information quantique va utiliser les propriétés particulières de la mécanique quantique, comme le non-clonage ou l'intrication, dans le domaine de l'information.

1.1 Information quantique

Un siècle après le début de la révolution quantique introduite par Einstein, la révolution de l'information quantique en est encore qu'à ses prémices. Comme vu déjà auparavant, du point de vue de la physique quantique, le monde est bien différent de ce que nous expérimentons dans la vie classique de tous les jours. Parmi les propriétés, nous avons en lien avec l'information quantique :

- une mesure d'un état quantique inconnu ne peut être effectuée en étant certain de ne pas perturber le système,
- les systèmes intriqués et leurs corrélations à distances,
- un état quantique quelconque ne peut être parfaitement copié,
- un état quantique ne peut être mesuré précisément et simultanément selon deux « directions » non orthogonales.

Au premier regard, ces propriétés peuvent nous paraître négatives par rapport à ce que nous expérimentons tous les jours. Cependant, nous verrons qu'en les utilisant intelligemment, ces propriétés peuvent se révéler très intéressantes et utiles pour certaines applications.

L'information quantique est nommée par analogie à l'information classique. Actuellement, l'information est enregistrée sous forme de *bits* 0 et 1. Classiquement, l'information est représentée par un objet macroscopique. Par exemple, pour transmettre des données de manière optique, les *bits* 0 et 1 sont représentés par deux intensités correspondant à de grands nombres de photons. Par contre, quantiquement, l'information peut être inscrite dans un photon unique par exemple. Ces unités d'information quantique sont appelées *qubits*, pour *quantum bit*. Les propriétés des *qubits* sont plus étendues que celle des *bits* classiques. Ils peuvent être dans les états $|0\rangle$ et $|1\rangle$, mais aussi en superposition $|0\rangle+|1\rangle$.

Par exemple, nous pouvons utiliser des photons uniques pour la cryptographie. La cryptographie consiste à échanger des données secrètes entre deux parties distantes. Cryptographie *quantique* signifie que la sécurité repose sur les lois de la physique quantique. En fait, la cryptographie quantique est utilisée pour échanger une clé secrète utilisée dans certains protocoles cryptographiques. Ainsi, nous devrions plutôt parler de distribution quantique de clés.

Pour l'échange de la clé secrète, l'émetteur, Alice, va envoyer une série de photons uniques en codant l'information dans une propriété de ces derniers (polarisation, phase, ...). Le récepteur, Bob, choisit une base de mesure et mesure ces photons. Alice et Bob doivent trouver certaines corrélations entre les données envoyées et reçues. Une espionne, Eve, (par rapprochement avec *eavesdropper*, oreille indiscrète, en anglais) va tenter d'obtenir la clé. Pour faire cela, elle mesure les photons entre Alice et Bob, elle peut alors être détectée. Elle va en effet introduire des perturbations lors de la mesure d'états quantiques inconnus. Les corrélations entre Alice et Bob seront donc réduites. Ainsi, avec les protocoles de distribution quantique de clés, la vérification de la confidentialité de l'échange repose sur les propriétés de la mécanique quantique, et pas sur de la complexité mathématique, par exemple, la décomposition de grands nombres en facteurs premiers, comme c'est le cas pour la cryptographie classique.

La distribution quantique de clés est le premier domaine de l'information quantique qui devrait trouver une application concrète dans la vie de tous les jours [9, 10]. Mais l'informa-

tion quantique pourrait connaître d'autres applications comme les ordinateurs quantiques. Pour ces derniers, l'intrication et la superposition quantique sont utilisées. La puissance de calcul augmentera, accélérant le calcul de certains problèmes par rapport aux ordinateurs classiques. Par exemple, un ordinateur quantique pourrait être utilisé pour des simulations quantiques ou pour la recherche de facteurs premiers de grands nombres. Pour le dernier cas, les calculs seraient exponentiellement plus rapides qu'avec les algorithmes actuels pour les ordinateurs classiques. Ainsi, cela permettrait de casser certains protocoles classiques de cryptographie utilisant de grands nombres premiers. Toutefois, bien que de premières expériences aient été faites, il reste de nombreuses étapes avant la réalisation d'un système pleinement fonctionnel.

1.2 Cette thèse

Dans cette thèse en physique expérimentale, nous allons voir comment les interférences quantiques nous permettent de « jouer » avec la physique. Elle se divise en deux parties bien distinctes : la première très appliquée traite de la distribution quantique de clés ; la seconde plus fondamentale concerne l'intrication à hautes dimensions. La première partie nous permettra de voir de manière concrète comment des propriétés fondamentales de la matière peuvent être utilisées pour une application dans la vie de tous les jours ou presque. Nous verrons que cela repose sur des idées très simples qui de manière surprenante ont mis de longues décennies avant d'apparaître.

Dans le chapitre 2, nous verrons l'implémentation du système de cryptographie dit *plug&play*, un système auto-aligné et auto-stabilisé, sur une distance de 67 km. Le contrôle d'interférences quantiques permet de s'assurer de la sécurité de l'échange de clés. Plus concrètement, cette expérience avait comme but de réaliser et tester un prototype « complet » de distribution quantique de clé. Le développement d'un tel système nécessite une intégration plus poussée que pour les expériences de laboratoire pour lesquelles nous n'avons pas de contraintes de place. Le développement terminé, nous avons testé ce système sur différentes fibres optiques installées dans un réseau de télécommunication standard. Par la suite, ce prototype a été repris et développé et est aujourd'hui commercialisé [9].

Toujours dans la partie très appliquée de cette thèse, le chapitre 3 présente l'implémentation d'un nouveau protocole de distribution quantique de clé. La sécurité de ce protocole repose sur la cohérence et les interférences quantiques. Ce nouveau protocole permet de supprimer certaines limitations du système *plug&play*. Il doit permettre d'obtenir des taux de clé secrète plus élevés et son implémentation devrait être plus facile. Une première expérience de principe sera présentée. Une seconde expérience plus complète sera aussi exposée, ainsi que les développements futurs.

Pour la dernière partie de cette thèse décrite dans le chapitre 4, nous avons fait une expérience de prospective. Cette expérience a été effectuée afin d'étudier la création et la détection d'interférences à hautes dimensions, dimensions supérieures à deux. L'intrication sera faite en superposition temporelle ou en *time-bin*. Les phénomènes d'interférences à hautes dimensions permettent d'obtenir des effets différents de ceux observés à deux dimensions. Dans cette dernière partie de thèse, nous avons étudié un système quantique avec une perspective fondamentale, toutefois, cela pourrait éventuellement par la suite être utilisé dans le champ de l'information quantique.

Chapitre 2

Cryptographie quantique *plug&play* sur 67 km

2.1 Introduction à la cryptographie

2.1.1 Cryptographie classique

L'art de transférer secrètement des données a intéressé les humains depuis très longtemps. Une très intéressante histoire des codes secrets est faite dans [11]. Probablement, la première tentative pour communiquer de manière secrète était d'utiliser la stéganographie (du grec « *steganos* », couvert, et « *graphein* », écrire). Avec cette technique, le message peut par exemple être caché sous des couches de cire ou sous la coquille d'un oeuf cuit dur. La principale faiblesse de cette manière de communiquer secrètement découle du fait que, si le message est découvert, alors il est directement intelligible par la personne l'interceptant.

La cryptographie (du grec « *kruptos* », caché, et « *graphein* », écrire comme vu précédemment) permet de combler cette faiblesse. Dans ce cas, la signification du message est cachée. Alors si quelqu'un intercepte le message, il doit parvenir à casser le code utilisé pour crypter le message afin d'en obtenir la signification. Le principe de la cryptographie est présenté sur la figure Fig. 2.1. Du côté de l'émetteur, Alice par convention, un algorithme permet de crypter un message clair à l'aide d'une clé. Le message codé est envoyé au récepteur, Bob par convention, par un canal public. Bob, grâce à un algorithme et une clé adéquate, peut retrouver le message clair. L'espionne, Eve par convention, va essayer d'intercepter et surtout de déchiffrer le message codé.

En cryptographie, nous avons le choix d'utiliser des algorithmes asymétriques ou symétriques. Pour les algorithmes asymétriques ou à clé secrète, les clés sont différentes pour le cryptage et le décryptage. Bob prend une clé privée et secrète à partir de laquelle, il calcule une clé publique. Bob envoie la clé publique à Alice. Alice code le message avec un algorithme utilisant la clé publique et envoie le message codé à Bob. Bob retrouve le message clair grâce à un algorithme utilisant la clé privée. La sécurité de ce type d'algorithmes repose sur la complexité de calculs grâce à l'utilisation de fonctions $f(x)$ dites à sens unique. Par définition d'une telle fonction, il est facile de calculer $f(x)$ à partir de x. Par contre, il est plus difficile de retrouver x à partir de $f(x)$, le temps nécessaire au calcul croît de manière exponentielle avec le nombre de *bits* à l'entrée. Un exemple simple est le suivant : la

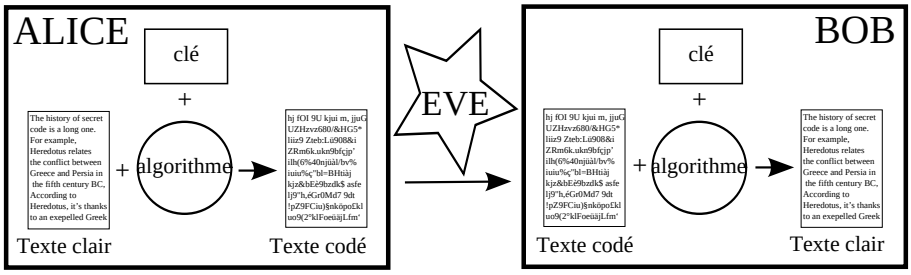


FIGURE 2.1 – *Cryptographie. L'émetteur, Alice, utilise un algorithme et une clé pour chiffrer un message clair. Le message crypté est envoyé au récepteur, Bob. Ce dernier utilise un algorithme et une clé pour retrouver le message clair. L'espionne, Eve, tente d'obtenir le message codé et surtout de trouver sa signification.*

multiplication $73 \times 97 = 7081$ se calcule facilement. Mais l'inverse, la factorisation de 7081 prend plus de temps. Le problème avec ce type d'algorithme est que la sécurité n'est pas prouvée, mais repose simplement sur de la complexité de calcul.

Pour les algorithmes symétriques ou à clé secrète, la même clé est utilisée pour le cryptage et le décryptage. La sécurité de ces protocoles repose également sur la complexité de calcul excepté pour un : le protocole *one-time pad* ou protocole à masque jetable [12] (FIG. 2.2). Ce protocole est prouvé sûr, c'est d'ailleurs le seul actuellement. Supposons que le message est écrit sous forme de données binaires, *bits* 0 et 1. La clé utilisée pour coder et décoder doit être une séquence aléatoire de *bits* 0 et 1 et de longueur identique au texte clair (le message à encoder). Pour crypter le message, Alice additionne *bit* à *bit* modulo 2 les *bits* du message et de la clé. Le message crypté, une séquence de *bits* aléatoire et sans information, est envoyé à Bob. Pour retrouver le message clair, il suffit à Bob de faire une addition *bit* à *bit* modulo 2 entre le message crypté et la même clé. Si le protocole est appliqué de manière correcte, clé aléatoire de longueur identique au message, et surtout, utilisation unique de la clé, alors le protocole à masque jetable est prouvé sûr.

Le point critique de ce protocole est l'échange de la clé entre Alice et Bob. À l'heure actuelle, ces échanges de clés se font, par exemple, avec des clés gravées sur des CDs ou DVDs. Il faut alors transférer physiquement les CDs ou DVDs d'Alice à Bob. Cela n'est pas très pratique. Il faut soit qu'Alice et Bob se rencontrent, soit faire confiance à une tierce personne se déplaçant d'Alice à Bob. La cryptographie quantique va permettre l'échange de la clé de manière sécurisée.

2.1.2 Cryptographie quantique

En 1984, un premier papier est publié sur la cryptographie quantique par Bennett et Brassard [13], bien qu'une idée proche est présente plus tôt avec Wiesner [14]. Cinq ans plus tard, la première expérience est réalisée dans l'air sur une distance de 32 cm [15]. D'autres protocoles ont été proposés par Bennett *et al.* [16], Ekert *et al.* [17] entre autres. Ce ne sont que quelques papiers, d'une longue série traitant du sujet. Une revue récente de cryptographie quantique se trouve dans [18]. Comme dit précédemment, plutôt que de cryptographie quantique, nous devrions parler de distribution quantique de clés, car ces protocoles ne font que distribuer une clé chez Alice et Bob. Cette clé est ensuite employée dans un algorithme de cryptage, idéalement, le protocole à masque jetable pour avoir un système parfaitement sûr.

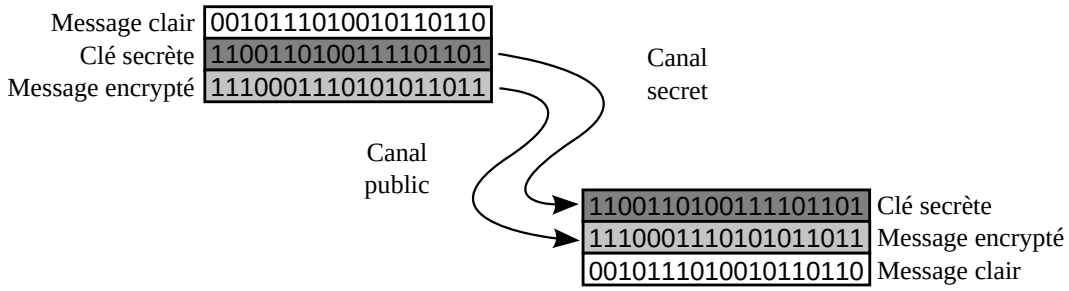


FIGURE 2.2 – *Protocole one-time pad ou à masque jetable. Pour crypter, le message clair est additionné bit à bit modulo 2 à une clé secrète aléatoire de longueur identique au message. La clé doit être transmise de manière sécurisée, alors que le message crypté peut être transmis sur un canal public. Pour retrouver le message clair, Bob additionne bit à bit modulo 2 la clé secrète et le message crypté. La preuve a été faite que ce protocole est sûr [12].*

De plus, si nous avons un doute sur la sécurité lors de l'échange de la clé (voir ci-dessous), aucune information n'est perdue, car la clé ne contient aucune information.

Comme pour l'échange d'information classique, des photons peuvent être utilisés pour l'échange quantique de la clé entre Alice et Bob. Cependant dans ce dernier cas, nous utilisons des photons individuels. L'information sera codée dans l'une ou l'autre des propriétés des photons, par exemple, la polarisation, la phase ou le temps. Par analogie avec l'information classique, ces états sont appelés *qubit* pour *quantum bit*. La sécurité va reposer sur le fait qu'Eve ne peut pas copier l'état quantique de ces photons (théorème de non-clonage [19, 20]), ni les mesurer sans les perturber.

Pour comprendre cela, étudions le protocole cryptographique BB84, proposé par Bennett et Brassard [13]. Ce protocole utilise quatre états quantiques formant deux bases maximalement conjuguées. Les *qubits* sont par exemple codés dans la polarisation des photons : horizontale (H) et verticale (V) pour une base ; et +45 ° (+) et -45 ° (-) pour l'autre base. La valeur 0 est associée aux polarisations H et + et la valeur 1 à V et -. Alice envoie une séquence de photons uniques en choisissant aléatoirement la polarisation pour chaque photon. Bob mesure les photons en choisissant aléatoirement les bases H/V ou +/-. Lorsque la base de mesure choisie est compatible avec les photons envoyés (H/V pour état H ou V, par exemple), alors le résultat est déterministe, sinon il est aléatoire (?) (TAB. 2.1). À ce moment, Alice et Bob partagent une clé brute. En comparant les bases de mesure et les états envoyés, Alice et Bob génèrent la clé dite tamisée ou *sifted* en ne conservant que les résultats compatibles.

Pour obtenir la clé, classiquement, une espionne, Eve, ferait simplement une copie de l'information envoyée. Quantiquement, la copie des *qubits* ne peut pas se faire de manière parfaite et avec probabilité 1, selon le théorème de non-clonage [19, 20]. Seules des des copies imparfaites ou/et avec probabilité inférieure à 1 sont possibles, voir [21], ou [22] pour une revue récente du clonage quantique. Ainsi, Eve n'aura qu'une information partielle et de plus elle sera détectée.

Pour mieux comprendre la sécurité du protocole, considérerons une attaque toute simple du protocole BB84 dite *interception-renvoi*. Eve se place entre Alice et Bob. Elle effectue une mesure analogue à celle de Bob, elle mesure les photons dans une des deux bases, et elle renvoie à Bob les photons selon la polarisation mesurée. Lorsqu'Eve utilise une base compatible avec les photons envoyés par Alice (50 % des cas), elle obtient toute l'information.

Base Alice	État Alice	*bit* logique Alice	Base Bob	Mesure Bob	*bit* logique Bob
H/V	H	0	H/V	H	0
H/V	H	0	+/-	?	?
H/V	V	1	H/V	V	1
H/V	V	1	+/-	?	?
+/-	+	0	+/-	+	0
+/-	+	0	H/V	?	?
+/-	-	1	+/-	-	1
+/-	-	1	H/V	?	?

TABLE 2.1 – *Protocole BB84 en polarisation. Les polarisations horizontale (H), verticale (V), +45° (+) et -45° (-) peuvent être envoyées aléatoirement. H, + codent 0 et V, - codent 1. Les deux bases sont H/V et +/-. Pour des bases de mesure compatibles, le résultat est déterministe (0 ou 1), alors qu'il est aléatoire pour des bases incompatibles (?).*

Le photon, qu'elle renvoie à Bob, a la bonne polarisation. Par contre lorsqu'elle utilise une base incompatible, le résultat de sa mesure est dans ce cas aléatoire, et la polarisation orientée à $\pm 45\,^{\circ}$ par rapport à celle initiale. Ainsi, si Bob utilise une base compatible avec le photon initial d'Alice, il verra une erreur dans 50 % de cas. Le taux total d'erreurs de *bit* quantique (*QBER*) entre les clés tamisées d'Alice et Bob est alors de $0.5 \times 0.5 = 25\,\%$.

En regardant le taux d'erreurs dans les corrélations attendues entre Alice et Bob, ils peuvent s'assurer de la confidentialité de la clé partagée. Si le taux d'erreurs est trop élevé, alors la clé est jetée, mais aucune information n'est perdue, car la clé est une simple séquence aléatoire sans information.

Dans la réalité, même sans espion, il y aura toujours un certain *QBER* dans la clé tamisée à cause des imperfections expérimentales. Quelle que soit leur cause, elles doivent être supprimées avec un processus classique de correction d'erreurs. Alice et Bob ont alors des clés identiques. Cependant, il est possible qu'Eve ait obtenu une certaine information, soit d'une attaque, soit du processus de correction d'erreurs qui implique une communication classique. Il faut alors appliquer une autre procédure classique : l'amplification de confidentialité. Ainsi, l'information d'Eve est réduite à un niveau arbitrairement bas. La dernière phase du traitement est l'authentification afin qu'Alice et Bob soient certains qu'ils communiquent bien l'un avec l'autre.

Il est important de noter que sous certaines conditions, *QBER* inférieur à une valeur limite, pertes de la fibre Alice-Bob inférieures à une certaine limite, essentiellement, il est possible d'obtenir une clé secrète nette entre Alice et Bob [23, 24]. Ainsi en utilisant la distribution quantique de clé pour échanger une clé, puis le protocole à masque jetable, l'échange d'information peut être effectué de manière totalement sécurisée.

2.2 Introduction *plug&play*

Cette expérience est la suite de plusieurs expériences décrites dans [25, 26, 27]. Le but de cette expérience était d'intégrer le plus possible le système développé précédemment, afin qu'Alice et Bob soient mis dans des boîtiers facilement transportables et utilisables dans des centraux de télécommunication. Le système construit effectue l'échange de la clé brute, c'est-à-dire, il

s'arrête avant le processus classique de réconciliation (correction d'erreurs, amplification de confidentialité, authentification). Toutefois, id Quantique a repris le système et l'a développé afin d'avoir un système commercial et complet de distribution de clé quantique [9]. Une autre entreprise a développé un système similaire [10].

Le système *plug&play* fonctionne avec des impulsions cohérentes atténuées. Ainsi, nous n'utilisons pas de source de photons uniques comme vu précédemment. Le nombre de photons par impulsions suivra une distribution de Poisson avec une valeur moyenne $\mu < 1$. Il est toutefois démontré que de telles sources permettent d'échanger des données de manière sécurisée [28, 29, 30].

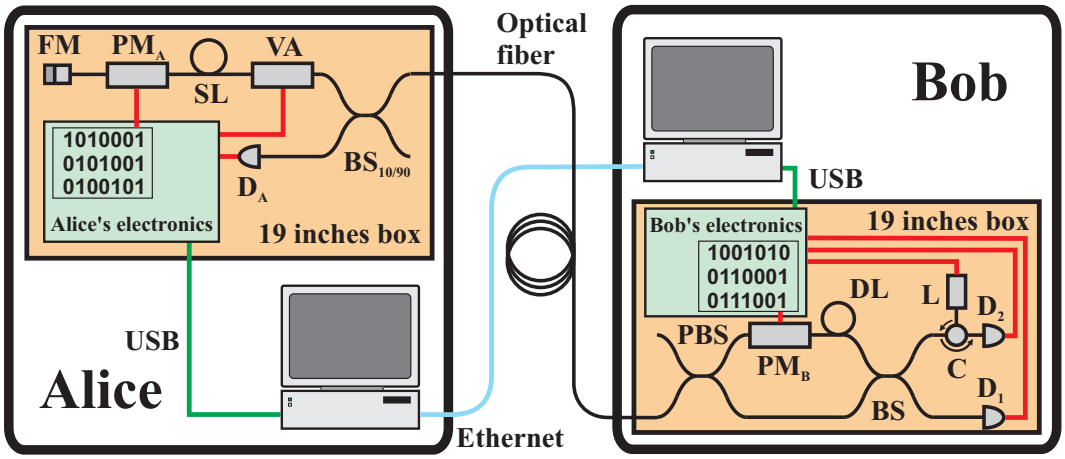


FIGURE 2.3 – *Implémentation du système plug&play. L : laser ; C : circulateur ; BS : coupleur ; DL : ligne de délai ; PM : modulateur de phase ; PBS : séparateur de polarisation ; D_1 et D_2 : photodiodes avalanche InGaAs/InP ; D_A : photodiode pré-amplifiée ; VA : atténuateur variable ; SL : ligne de stockage ; FM : miroir de Faraday. Pour une explication détaillée du fonctionnement, voir le texte.*

Le schéma de principe se trouve sur la figure FIG. 2.3. Bob envoie des impulsions intenses. En arrivant sur le coupleur 50/50 BS, une moitié des photons passe par le bras court de l'interféromètre et l'autre moitié passe par le bras long contenant le modulateur de phase PM_B et sa polarisation est tournée de 90°. La seconde impulsion est moins intense que la première à cause des pertes dans le modulateur d'intensité du bras long. Les impulsions sont envoyées à Alice, où elles sont réfléchies puis atténuées, afin de réduire le nombre moyen de photons à $\mu/2$ pour la seconde impulsion. La seconde impulsion est également modulée avec une phase 0, $\pi/2$, π ou $3\pi/2$, par le modulateur de phase PM_A.

Lorsque les photons reviennent chez Bob, la première impulsion passe par le bras long et la seconde impulsion passe par le bras court. Cela est dû au fait qu'avec un miroir de Faraday, quand la lumière revient, sa polarisation est orthogonale à celle originale et donc, les impulsions passent par les chemins opposés au retour sur le séparateur de polarisation. Bob choisit la base de mesure en appliquant une phase 0 ou $\pi/2$. En fonction des phases appliquées par Alice et Bob, la détection se fait de matière déterministe (base compatible) ou aléatoire (base incompatible), sur les photodiodes à avalanches D_0 ou D_1.

Un problème du système *plug&play* est la rétrodiffusion Rayleigh. Pour l'éviter, les impulsions sont envoyées sous forme de trains, qui en arrivant chez Alice remplissent la ligne de stockage SL, placée après l'atténuateur variable. Bob ouvrira ces détecteurs uniquement lorsque les

trains d'impulsions reviennent. Puis, Bob envoie un nouveau train d'impulsions.

Les principaux avantages d'une telle configuration sont que le système est auto-aligné (un seul interféromètre) et auto-stabilisé (grâce au miroir de Faraday).

2.3 Implémentation du système

La configuration (FIG. 2.3) pour l'expérience est presque la même que celle utilisée dans [27]. Il y a cependant eu quelques modifications dans le choix des composants :

- des composants avec fibres à maintien de polarisation sont utilisés chez Bob. Des photons entrant dans ce type de fibres, avec une polarisation bien alignée selon un des axes principaux de la fibre, suivront cet axe. Ainsi, il n'est plus nécessaire d'avoir des contrôleurs de polarisation afin de tirer parti au maximum de la configuration avec le séparateur de polarisation et le miroir de Faraday.
- pour minimiser les pertes sur la ligne de transmission, une fibre optique standard, la longueur d'onde utilisée est de 1550 nm (1310 nm dans l'expérience précédente).
- le système fonctionne à une fréquence de répétition $\nu = 5$ MHz, 2.5 MHz précédemment
- une électronique dédiée avec de la logique programmable (FPGA) a été développée afin de pouvoir contrôler l'ensemble du système
- la partie logicielle a été développée pour le contrôle du système et l'échange de la clé. La communication entre la partie matérielle et l'ordinateur externe est faite par un lien USB. La communication USB a été développée par la société Ellisys [31].

Pour le reste, l'implémentation est assez similaire. Nous utilisons des détecteurs InGaAs/InP en mode avalanche ou Geiger. L'efficacité de détection η_B vaut environ 10 % avec une probabilité de bruit de l'ordre 10^{-5} par ns. Pour diminuer, les coups de bruit, nous n'ouvrons que des portes de détection de 2.5 ns à la fréquence de répétition ν. Pour éviter les problèmes d'échos d'avalanche [32, 33], nous appliquons des temps-morts sur les détecteurs, c'est-à-dire nous laissons la tension en dessous de la tension de claquage un certain temps. Pour éviter la rétrodiffusion Rayleigh, nous envoyons des trains de 480 impulsions à la fréquence de répétition ν. Ainsi, nous n'excédons pas la capacité de la ligne de stockage SL de longueur $l_{SL} = 10$ km.

2.4 Paramètres clé

Dans [34], les paramètres importants sont calculés. Nous obtenons pour le taux de clé brut R_{brut} :

$$R_{brut} = q\nu\mu t_{AB} t_B \eta_B \eta_{duty} \eta_\tau \tag{2.1}$$

où :

- q dépend du protocole (0.5 pour BB84, car dans la moitié des cas les bases sont incompatibles entre Alice et Bob)

- t_{AB} est la transmission entre Alice et Bob
- t_B est la transmission chez Bob
- $\eta_{duty} = \frac{l_{SL}}{l_{AB}+l_{SL}}$ tient compte du fait que les photons sont émis sous forme de train avec un ligne de stockage (l_{AB} : distance Alice-Bob)
- $\eta_\tau = \frac{1}{1+\nu p_{det}\tau}$ permet de prendre en considération le temps-mort τ, fixé à $4\,\mu$s dans l'expérience (p_{det} : probabilité de détection par porte).

Le *QBER* est défini par :

$$QBER = \frac{mauvaises\,détections}{détections\,totales} = QBER_{opt}+QBER_{cs}+QBER_{échos}+QBER_{parasite} \quad (2.2)$$

où :

- $QBER_{opt}$ est la probabilité qu'un photon atteigne le mauvais détecteur à cause de problèmes d'alignement de polarisation et de stabilité de la ligne
- $QBER_{cs} \cong \frac{p_{cs}}{\mu t_{AB} t_B \eta_B}$ est la probabilité de coups sombres par porte p_{cs} divisée par la probabilité de détection
- $QBER_{échos} \cong \sum_{n=0}^{n=\frac{1}{p_{det}}} p_{échos}\left(\tau + n\frac{1}{\nu}\right)$ est la somme des probabilités d'échos d'avalanche entre deux détections ($p_{echos}(t)$: probabilité d'échos d'avalanche par porte de détection un temps t après une première détection)
- $QBER_{parasite}$ est le taux d'erreurs induit par de la lumière parasite, essentiellement la rétro-diffusion Rayleigh, pour la configuration *plug&play*. Cependant, la ligne de stockage SL permet d'éviter ce problème.

La visibilité est un paramètre important pour ce protocole, comme pour d'autres, et elle peut être exprimée en fonction de $R_{correct}$ and R_{faux} les taux de détections correctes et fausses respectivement :

$$V = \frac{R_{correct} - R_{faux}}{R_{correct} + R_{faux}} \quad (2.3)$$

ainsi nous pouvons écrire pour le $QBER_{opt}$:

$$QBER_{opt} = \frac{1-V}{2} \quad (2.4)$$

Le dernier paramètre utile est une évaluation du taux de clé nette :

$$R_{net} = \eta_{dist} R_{brut} \cong (I_{AB} - I_{AE})\frac{I'_{AB}}{I_{AB}} R_{brut} \quad (2.5)$$

où I_{AB} et I_{AE} sont les informations mutuelles Alice-Bob et Alice-Eve respectivement, I'_{AB} est l'information mutuelle Alice-Bob après correction d'erreurs.
L'évaluation de ces différentes informations est donnée dans [34].

2.5 Résultats expérimentaux

Le système a été testé dans un réseau de télécommunication standard. Les tests ont été faits sur des fibres sous-lacustre, terrestre ou aérienne de 8.7 à 67.1 km. Dans la table TAB. 2.2, nous voyons que la visibilité est supérieure à 99 % et donc selon (2.4) le $QBER_{opt}$ sera inférieur à 0.5 %. Donc, ni les vibrations possibles pour des fibres terrestres proches de routes, ni le vent pour les fibres aériennes ne perturbent véritablement la stabilité interférentielle du système *plug&play*. Avec un brouilleur de polarisation et une bobine de 25 km de fibre, la visibilité est passée de 99.7 % à 99.5 % et 98.0 % avec des fréquences de brouillage de 40 et 100 Hz. Cette fréquence correspond au nombre de tours par seconde que le vecteur de polarisation effectue dans la sphère de Poincaré.

Fibre	Longueur [km]	Pertes [dB]	Visibilité [%]
Genève-Nyon (sous-lacustre)	22.0	4.8	99.70 ± 0.03
Genève-Nyon (terrestre)	22.6	7.4	99.81 ± 0.03
Nyon-Lausanne (terrestre)	37.8	10.6	99.63 ± 0.05
Genève-Lausanne (sous-lacustre) A	67.1	14.4	99.62 ± 0.06
Genève-Lausanne (sous-lacustre) B	67.1	14.3	99.66 ± 0.05
Ste Croix (aérien) A	8.7*	3.8	99.70 ± 0.01
Ste Croix (aérien) B	23.7*	7.2	99.71 ± 0.01

TABLE 2.2 – *Résultats de visibilité pour différentes configurations. * La partie de fibre aérienne effective faisait 2×2.5* km. *La différence entre les deux expériences provient de l'ajout d'une bobine de 15* km *entre les deux segments aériens.*

Ensuite, nous avons réalisé des échanges quantiques de clés pour les mêmes fibres TAB. 2.3. Le taux de clé brute a été mesuré entre 0.15 à 6.3 kHz. Le QBER varie entre 2.0 % et 6.1 %. Nous avons également évalué le taux de clé nette. pour les possibilités d'attaque d'Eve, nous avons considéré les mêmes hypothèses que dans [35] :

- pas de mesures du nombre de photons sans perturbation,
- pas de mémoire quantique,
- QBER dans la limite statistique estimée selon (2.2).

Nous estimons un taux de clé net entre 44 Hz et 4.34 kHz.

Fibre	Longueur [km]	Clé [kbit]	$R_{brute}[kHz]$	QBER [%]	$R_{nette}[kHz]$
Genève-Nyon (sous-lacustre)	22.0	27.9	2.06	2.0±0.1	1.51
Genève-Nyon (terrestre)	22.6	27.5	2.02	2.1±0.1	1.39
Nyon-Lausanne (terrestre)	37.8	25.1	0.50	3.9±0.2	0.26
Geneva-Lausanne (sous-lacustre) A	67.1	12.9	0.15	6.1±0.4	0.044
Geneva-Lausanne (sous-lacustre) B	67.1	12.9	0.16	5.6±0.3	0.051
Ste Croix (aérien) A	8.7	63.8	6.29	3.0±0.1	4.34
Ste Croix (aérien) B	23.7	117.6	2.32	3.0±0.1	1.57

TABLE 2.3 – *Résultats de distribution quantique de clés pour différentes configurations avec* $\mu = 0.2$. *Le taux de clé nette* R_{nette} *est calculé à partir de taux de clé brute* R_{brute}, *du QBER et de la formule (2.5).*

2.6 Conclusion

Nous avons donc distribué des *qubits* sur une distance supérieure à 67 km avec un taux de clé net estimé de 50 Hz.

Comme cela a déjà été écrit plus haut, ce prototype a été repris et développé afin d'obtenir un produit qui est maintenant commercialisé. Il est assez étonnant de voir comment des propriétés fondamentales et très simples de la physique peuvent être utilisées à un niveau très appliqué. Mais ce qui est encore plus surprenant est qu'il ait fallu des dizaines d'années pour voir apparaître la cryptographie quantique, alors qu'un étudiant en physique peut comprendre le principe après son premier cours de mécanique quantique.

Chapitre 3

Cryptographie simple et rapide

3.1 Introduction

Dans le chapitre 2, nous avons vu un système de distribution de clé quantique ayant donné lieu à un système commercial [9]. Malgré ses avantages indéniables, ce système présente quelques faiblesses. Premièrement, les impulsions faisant un aller-retour Bob-Alice, Alice-Bob, et la nécessité d'envoyer des trains finis d'impulsions, font que le débit maximal sera limité. Du point de vue de la complexité, le système *plug&play* nécessite un nombre assez élevé de composants. Il est nécessaire de faire des choix actifs chez Alice et chez Bob pour choisir les états et la base de mesure respectivement.

Nous avons alors cherché un protocole qui soit le plus pratique en vue d'une application. Ce protocole doit satisfaire les conditions suivantes :

- le système doit permettre une implémentation facile avec des composants standards utilisés en télécommunications,
- la sécurité doit reposer sur des propriétés de la physique quantique, comme la cohérence quantique par exemple.

Nous avons donc développé un nouveau protocole satisfaisant ces propriétés : le protocole Coherent One Way (COW). Il fonctionne en aller simple, avec des impulsions cohérentes faibles à 1550 nm et un codage des *qubits* en temps. À l'entrée de Bob, les photons peuvent prendre l'un ou l'autre de deux chemins. Sur le premier, la *ligne de données*, une simple mesure du temps d'arrivée des photons permet de générer la clé. Sur le second, la *ligne de contrôle*, un interféromètre et des détecteurs permettent de vérifier la présence d'un espion. Notons qu'un système avec une *ligne de données* similaire a été développé [36].

3.2 Protocole

La figure Fig. 3.1 schématise ce nouveau protocole. Grâce à un laser suivi d'un modulateur d'intensité, Alice envoie une suite d'impulsions. Les impulsions sont soit vides (impulsion 0), soit avec un nombre moyen de photons $\mu < 1$ avec une distribution de Poisson (impulsion μ) (Fig. 3.2). Une séquence de deux impulsions $\mu - 0$ (ou $|\mu\rangle \otimes |0\rangle$) code le *bit* logique 0, alors que $0 - \mu$ (ou $|0\rangle \otimes |\mu\rangle$) code le *bit* logique 1. Notons qu'à cause de la composante du

vide des impulsions μ, les deux états ne sont pas orthogonaux. Alice doit également envoyer des séquences de deux impulsions $\mu - \mu$ (ou $|\mu\rangle \otimes |\mu\rangle$) pour des raisons de sécurité (voir ci-dessous). Ces séquences sont appelées *decoy sequences* ou *séquences leurre*, par référence aux *decoy states* introduits dans [28, 30]. Cependant, contrairement aux *decoy states*, les *decoy sequences* ne codent pas de *bits* logiques.

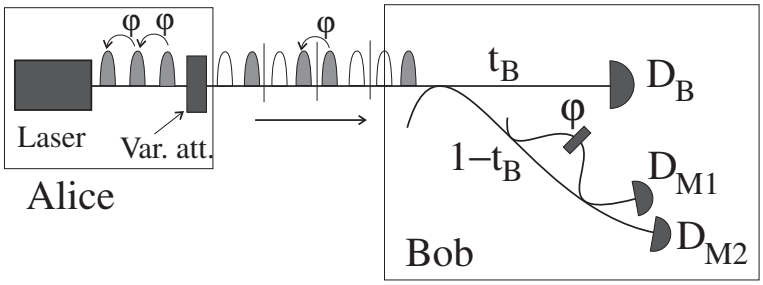


FIGURE 3.1 – *Protocole COW. Le détecteur D_B permet d'obtenir la clé en enregistrant le temps de détection. Les détecteurs D_{M_1} et D_{M_2} permettent de s'assurer de la cohérence entre impulsions μ successives et ainsi garantir la sécurité.*

Sur la *ligne de données* (détecteur $\mathrm{D_B}$), Bob doit pouvoir discriminer deux états non orthogonaux. Cela ne peut pas se faire de manière non ambiguë. La meilleure stratégie pour discriminer les séquences non orthogonales $\mu - 0$ et $0 - \mu$ et pour générer la clé, consiste à enregistrer les temps d'arrivée [37]. La *ligne de contrôle*, avec un interféromètre et les détecteurs $\mathrm{D_{M_1}}$ et $\mathrm{D_{M_2}}$, permet de mesurer la présence d'une espionne, en vérifiant la cohérence entre deux impulsions μ successives. L'interféromètre peut être aligné afin d'avoir des interférences destructives sur $\mathrm{D_{M_1}}$ et constructives $\mathrm{D_{M_2}}$, sans espion. S'il y a un espion, cela changera.

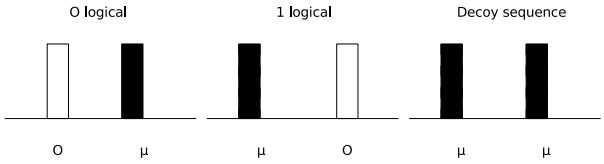


FIGURE 3.2 – *Codage des qubits pour le protocole Coherent One Way. La première impulsion est celle de droite. En plus des qubits 0 et 1, des decoy sequence sont envoyées pour des raisons de sécurité (voir* FIG. *3.3).*

En résumé, le protocole se déroule de la manière suivante :

- Alice envoie une longue séquence aléatoire de *bits* 0 et 1 avec probabilité $(1 - f)/2$ pour chacun d'entre eux et des *decoy sequences* avec probabilité $f << 1$
- Bob indique la *position* du *bit* pour les détections sur le détecteur de données $\mathrm{D_B}$ et les *temps* de détections exacts sur les détecteurs de contrôle $\mathrm{D_{M_1}}$ et $\mathrm{D_{M_2}}$
- Alice dit quelles détections correspondent à des *decoy sequences* et doivent être supprimées des résultats sur $\mathrm{D_B}$ (*sifting*)
- Alice évalue l'information d'Eve à partir de l'évaluation de la visibilité sur l'interféromètre

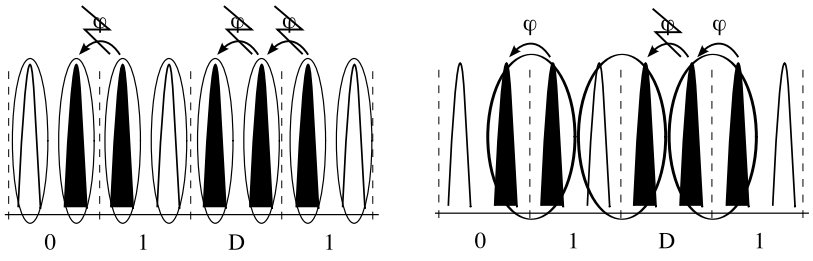
- finalement, Alice et Bob effectuent le travail classique de correction d'erreur, amplification de confidentialité et authentification.

3.2.1 Attaque d'Eve

Dans [37], une première étude de sécurité est présentée. Nous allons en résumer les grandes lignes. Eve peut effectuer une simple *attaque coupleur*, en enlevant une fraction $1-t$ des photons et en transmettant le reste à Bob sur une fibre sans pertes. Sur la fraction $1-t$, Eve effectue une mesure du temps de détection, car c'est la meilleure stratégie pour discriminer les deux *qubits* non orthogonaux. Ainsi, Eve obtient une fraction d'information $\mu(1-t)$ dont il faut tenir compte lors de l'amplification de confidentialité.

Avec les protocoles comme BB84 et bien d'autres, en tirant parti des impulsions contenant plus d'un photon et des pertes dans la ligne entre Alice et Bob, Eve peut obtenir de l'information sans introduire d'erreur. Ce sont les attaques *photon number splitting* [38, 39]. Ce type d'attaques se fait individuellement sur chaque impulsion. Eve compte les photons et en garde un s'il y a plus d'un photon et laisse passer les autres. Avec ce nouveau protocole, une telle attaque individuelle brise la cohérence entre impulsions μ successives, et cela induit des erreurs (FIG. 3.3(a)). Notons que pour ce protocole, cette attaque est équivalente à une attaque du type *interception-renvoi*.

Eve pourrait essayer un autre type d'attaque pour laquelle, elle fait une mesure cohérente en mesurant le nombre n de photons dans deux impulsions successives. Supposons qu'Eve se synchronise avec Alice et effectue cette attaque à cheval sur la séparation des *bits* logiques. Dans ce cas, elle ne brise pas la cohérence pour les séquences logiques 10 (ou impulsions $0-\mu-\mu-0$) et obtient une certaine information lors du processus de *sifting*, si elle mesure $n > 0$. Cependant avec les *decoy sequences*, elle brisera la cohérence et donc sera détectée (FIG. 3.3(b)).



(a) Attaque individuelle. (b) Attaque cohérente.

FIGURE 3.3 – *Brisure de cohérence. Les attaques sont représentées par les ovales. (a) Avec des attaques individuelles, la cohérence est brisée pour toutes les impulsions μ successives. (b) Pour une attaque cohérente sur deux impulsions successives, Eve n'est pas détectée excepté pour les decoy sequences.*

3.3 Implémentation

3.3.1 Expérience de principe

Lors d'une première expérience de principe [40], une séquence de huit impulsions a été envoyée de manière répétitive et l'enregistrement des données a été effectué de manière statistique à l'aide d'un *time-to-digital converter* (*TDC*) (Fig. 3.4). La séquence logique envoyée est D010, D pour *decoy sequence*.

Pour générer cette séquence, nous avons fabriqué une électronique spécifique. Nous avons entre autres utilisé un composant appelé sérialiseur. Cela nous permet de séparer le système en une partie fonctionnant à vitesse élevée avec des données en série et le reste travaillant plus lentement sur des données en parallèle. En effet, un sérialiseur fonctionne de la manière suivante. Nous entrons avec un nombre n de *bits* en parallèle à une fréquence F/n et une horloge rapide de fréquence F. À la sortie, les *bits* sortent l'un après l'autre à la fréquence F.

Dans le train de huit impulsions, le temps entre impulsions τ est défini par l'horloge C_1 fonctionnant à F=434 MHz. Ainsi, les *bits* logiques vont à 217 MHz dans la séquence (en négligeant la *decoy sequence*). L'horloge C_2 allant jusqu'à 600 kHz définit la fréquence de répétition de la séquence de 8 *bits*. Le signal à la sortie du sérialiseur passe par un préamplificateur, puis un amplificateur qui commande un modulateur d'intensité IM. Ainsi, cela module un laser continu à 1550 nm (CW laser) selon la séquence de 8-*bits*. L'atténuateur variable permet de régler le niveau moyen de photon μ à 0.5. En ajoutant 5 dB d'atténuation supplémentaire, nous simulons des pertes supplémentaires de 5 dB, correspondant à 25 km, pour une fibre avec des pertes de 0.2 dB/km. Le signal de synchronisation est envoyé directement avec un câble coaxial d'Alice à Bob.

Du côté de Bob, le signal de synchronisation est utilisé pour activer les deux détecteurs ainsi que le *time-to-digital converter*. Les portes sur les détecteurs font un peu plus de 20 ns de large. Ainsi, il est possible de détecter la séquence complète de 8 impulsions. Toutefois, il y a au maximum une détection par séquence et par détecteur à cause du temps mort du détecteur. L'interféromètre de contrôle est construit avec un coupleur 50/50 et deux miroirs de Faraday. Ainsi, il est automatiquement aligné en polarisation. Nous n'avons utilisé qu'un détecteur de contrôle D_M. Pour vérifier la visibilité, nous avons simplement fait varier la phase dans l'interféromètre en modifiant sa température.

Sur D_B, le taux brut de détection est de 17.0±0.1 kHz avec une efficacité de détection de 10 % et une probabilité de coups sombres de 2.5×10^{-5} par ns.

Sur D_B, le QBER est de 5.2±0.4 % dont 4 % venant du détecteur et le reste étant dû à une modulation imparfaite et au *jitter* des détecteurs. En variant la phase dans l'interféromètre, nous mesurons sur D_M une visibilité brute de 92 % et d'environ 98 % et soustrayant les coups sombres et les échos d'avalanche sur le détecteur D_B.

Conclusion de l'expérience de principe

Avec cette première expérience, nous avons démontré la faisabilité de ce nouveau protocole. Certaines améliorations pourraient être réalisées. Le taux de détection, et donc le taux de clé, pourraient être augmentés en envoyant des impulsions 0 ou μ de manière continue (amélioration du *duty cycle*), en optimisant f et t_B. Nous avons apporté certaines de ces améliorations

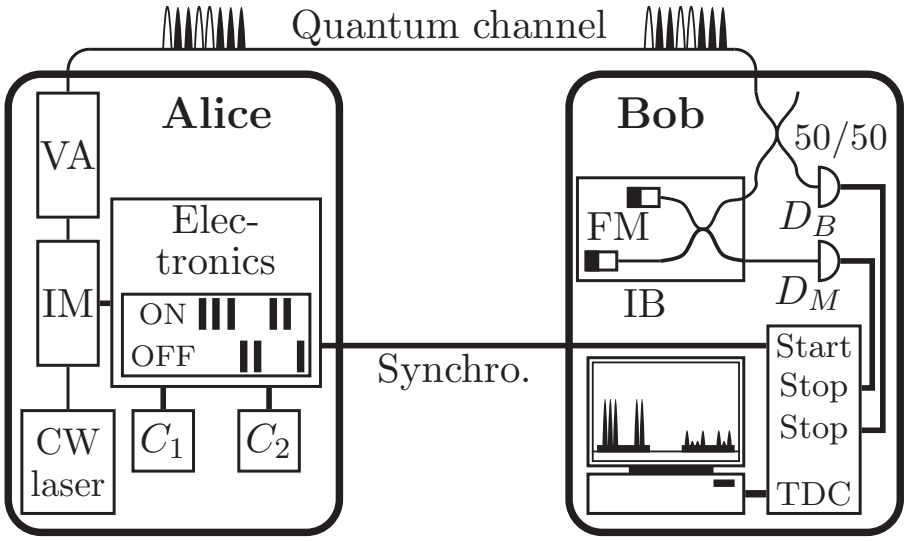


FIGURE 3.4 – *Expérience de principe. C_1 : horloge impulsions ; C_2 : horloge séquence ; IM : modulateur d'intensité ; VA : atténuateur variable ; FM : miroir de Faraday ; IB : boîte isolée ; D_B et D_M : détecteurs InGaAs/InP ; TDC : time-to-digital converter. Pour les détails de fonctionnement, voir texte.*

dans une seconde expérience.

3.3.2 Deuxième expérience

Après cette première, nous en avons commencé une seconde plus proche d'une implémentation complète du système (FIG. 3.5). Cette fois, Alice peut envoyer une séquence de 1 Mo d'impulsions, donc environ 0.5 Mo de *bits* logiques (en négligeant les *decoy sequences*). Depuis un ordinateur, les données sont chargées dans la mémoire M d'Alice par un port série. Ensuite, Alice peut envoyer cette séquence en boucle. Pour envoyer des données, grâce à de la logique programmable (CPLD), Alice lit les données dans la mémoire sur une largeur de bus de 16 *bits* à une fréquence de 760/16=47.5 MHz et les fournit à deux sérialiseurs de 8 *bits* mis en série. À la sortie des sérialiseurs, nous avons la séquence d'impulsions à une fréquence de 760 MHz et donc des *bits* logiques à 380 MHz. Les impulsions sortantes sont amplifiées (PA et A) et entrent dans le modulateur d'intensité IM qui module le laser continu (CW laser). L'intensité moyenne des impulsions μ est ajustée avec l'atténuateur variable VA. Parallèlement, grâce à une seconde fibre optique, un signal de synchronisation est envoyé par des modules *transceivers* SFP, utilisés en télécommunications classiques. Le signal de synchronisation n'est rien d'autre que l'horloge à laquelle, Alice enlève juste une impulsion. En détectant cette impulsion manquante, Bob génère un signal de *reset*.

Le compteur de 8 *bits* fonctionne à 760 MHz et permet de connaître le moment exact de la détection, donc la valeur logique. Lorsqu'une détection intervient, cela déclenche l'enregistrement de la valeur du compteur de 8 *bits* dans des registres R distincts, pour chacun des deux détecteurs, puis dans la logique programmable (CPLD). Ainsi, il est possible d'enregistrer des doubles détections. Un compteur de 6 *bits* dans le CPLD compte les débordements du compteur de 8 *bits*. Ensuite grâce au CPLD, les temps de détection sont envoyés dans un ordinateur à travers une carte d'acquisition avec 32 entrées digitales TTL. En fait, à chaque

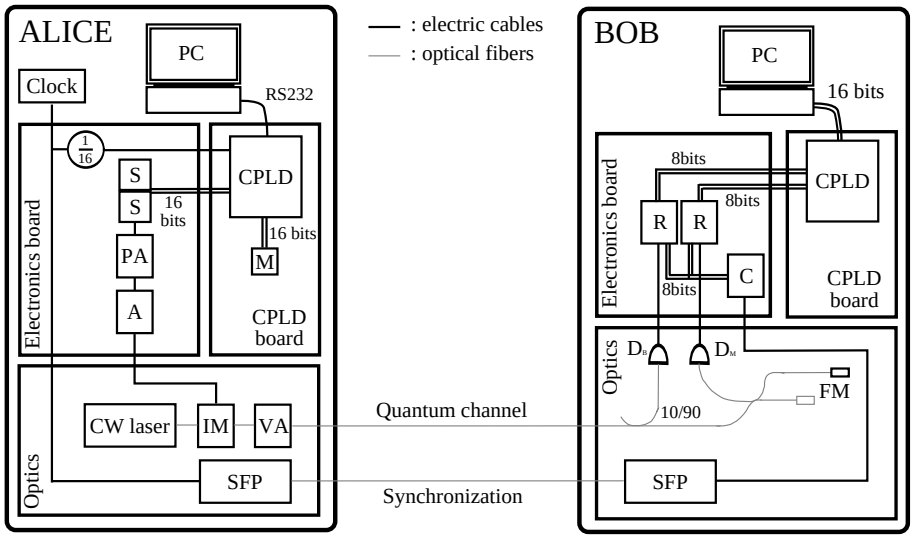


FIGURE 3.5 – *Seconde expérience. Clock : horloge fonctionnant à 760* MHz *; M : mémoire de 1* Mo *; CPLD : logique programmable ; S : sérialiseur ; PA : pré-amplificateur ; A : amplificateur ; IM : modulateur d'intensité ; VA : atténuateur variable ; SFP : modules transceiver ; D_B et D_M : photodiodes à avalanches InGaAs/InP ; FM : miroir de Faraday ; C : compteur de 8 bits fonctionnant à 760* MHz *; R : registres de 8 bits.*

acquisition, nous enregistrons les 14 *bits* du compteur total et un *bit* pour chaque détecteur afin de savoir lequel clique. Donc, nous enregistrons 16 *bits* par acquisition. En plus des détections, les débordements de compteur total de 8+6=14 *bits* sont transmis à l'ordinateur. Nous pouvons ainsi retrouver les temps absolus de détections depuis le signal de *reset*.

Pour contrôler le système, nous avons développé du côté d'Alice un programme permettant d'envoyer les données stockées dans la mémoire ou des séquences pré-définies. Du côté de chez Bob, nous avons fait un petit programme permettant d'enregistrer les données. Ainsi, nous avons pu effectuer des tests. Malheureusement, les résultats n'ont pas été totalement concluants. La partie d'Alice fonctionne bien. Nous pouvons charger le fichier que nous voulons en mémoire et utiliser ce fichier afin de moduler le laser continu. Pour vérifier cela, nous avons fait des tests avec différentes séquences que nous avons envoyées. Des mesures avec un oscilloscope nous ont permis de voir que nous modulions correctement le laser. Cependant, lorsque nous cherchons à enregistrer les données avec Bob, des problèmes apparaissent. Il arrive parfois, en général avec une probabilité inférieure à 1 % que le temps de détection de la détection $n+1$ est inférieur à celui de la détection n. Nous n'avons pas pu résoudre ces problèmes, mais espérons les résoudre dans le cadre du développement d'un nouveau système pour le projet SECOQC [41].

3.3.3 Développements futurs

Pour le projet de recherche européen SECOQC, nous devons réaliser un système fonctionnant en continu 24 heures sur 24, 7 jours sur 7 dans un réseau de télécommunication. Ce réseau qui va utiliser différents système de distribution quantique de clés [41], a pour but de construire un réseau de communication avec une sécurité basé sur la cryptographie quantique.

Pour faire le nouveau système, la partie de logique programmable actuelle (CPLD) va être

remplacée par des systèmes plus puissants (FPGA). Cela permettra d'utiliser les sérialiseurs et désérialiseurs internes aux FPGA. Cela devrait nous permettre de simplifier la construction du système et faciliter le réglage des délais entre les différents signaux. Comme cela avait été le cas pour le système *plug&play*, l'intégration devra être plus poussée que pour un développement standard fait en laboratoire. Il faudra pouvoir l'intégrer dans des boîtiers (19 pouces de large). La partie logicielle pour l'automatisation du système devra être fortement développée et fonctionner sur un système Linux dans un ordinateur embarqué. Le système devra permettre un échange de clé complet avec toute la phase classique de correction d'erreurs, amplification de confidentialité et authentification.

Les mauvaises performances des détecteurs sont un problème avec les systèmes fonctionnant à 1550 nm et encore plus lorsque le système fonctionne à une vitesse élevée. Les photodiodes InGaAs/InP actuelles ne permettent pas vraiment d'espérer des fréquences de détections supérieures à 100 kHz, à cause des temps morts nécessaires pour éviter les échos d'avalanche. De plus, le *jitter* peut devenir un problème avec un accroissement de la vitesse. Il y a cependant de nouveaux détecteurs qui apparaissent. Tout d'abord, il y a de nouveaux détecteurs InGaAs/InP [42, 43]. Ils pourraient avoir de meilleures caractéristiques, mais toutefois doivent être testés.

Autrement avec de la détection par conversion paramétrique, il est possible d'atteindre des fréquences de détection de quelques MHz [44, 45]. Cependant, si nous voulons avoir un système commercial, il faut encore améliorer la construction de ces détecteurs. Finalement, d'autres détecteurs possibles sont des détecteurs supraconducteurs. Dans ce cas, la fréquence de détection pourrait atteindre des GHz [46, 47], mais à des températures cryogéniques et donc cela rend une application peu aisée.

Lorsque ce problème de détection sera résolu, un autre problème va devenir de plus en plus important : le processus classique de réconciliation. Plus particulièrement, le processus de correction d'erreur deviendra critique. Il va falloir étudier comment optimiser cette phase afin que cela ne devienne pas le goulot d'étranglement.

Un dernier problème est la génération des nombres aléatoires pour moduler le laser. Nous avons besoin d'un générateur physique de vrais nombres aléatoires et pas uniquement un générateur de nombres pseudo aléatoires pour avoir une sécurité complète.

3.4 Conclusion

Le nouveau protocole de distribution quantique de clés a été implémenté dans une première expérience de principe. Pour la première expérience, les résultats ont été concluants. Pour la seconde expérience, les résultats n'ont été que partiellement concluants. Nous avons toutefois pu envoyer des *bits* logiques à une fréquence de 380 MHz. Nous avons réussi à les détecter, bien qu'il restait encore quelques problèmes. Néanmoins, nous n'avons pas trouvé de problèmes fondamentaux dans l'implémentation. De plus, cela nous a permis d'expérimenter de l'électronique rapide et de prendre conscience de certains problèmes pour des développements futurs.

Avec l'expérience acquise et des développements supplémentaires bien sûr, nous devrions pouvoir obtenir un système fonctionnant à une fréquence de plusieurs centaines MHz dans l'année à venir, puis à quelques GHz dans un futur assez proche.

Chapitre 4

Intrication à hautes dimensions

4.1 Introduction

Par rapport aux expériences précédentes, ce chapitre va présenter un sujet plus fondamental. Cette expérience est présentée avec une perspective d'*optique* quantique. Cependant, l'intrication à hautes dimensions pourrait être utilisée pour des expériences plus orientées vers de nouveaux protocoles d'*information* quantique. Par exemple, la distribution de clé quantique peut se faire avec une tolérance plus grande au bruit avec des dimensions élevées [48]. Il est également possible de réduire l'efficacité des détecteurs pour fermer l'échappatoire de détection dans le paradoxe EPR [49]. Des systèmes à hautes dimensions permettent une violation du réalisme local plus importante que les systèmes à deux dimensions [50] et avec une plus grande robustesse au bruit [51].

Commençons par introduire la conversion paramétrique spontanée, et faire un rappel sur l'intrication.

4.1.1 Conversion paramétrique spontanée

La figure Fig. 4.1 présente le processus non-linéaire de conversion paramétrique spontanée (SPDC) [52, 53]. À l'entrée du cristal, il y a un laser de pompe (ω_p, k_p) et à la sortie nous avons des photons *signal* (ω_s, k_s) et *idler* (ω_i, k_i). Les effets non-linéaires sont dus aux termes d'ordre supérieur de la susceptibilité, terme d'ordre deux $\chi^{(2)}$ dans notre cas. Pour obtenir des effets non-linéaires, il faut choisir de manière adéquate le laser et le cristal non-linéaire et l'orientation de son axe optique par rapport à la polarisation du laser. Il doit en effet y avoir conservation de l'énergie et de l'impulsion :

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i$$
$$\hbar\vec{k}_p = \hbar\vec{k}_s + \hbar\vec{k}_i$$

où ω_p, ω_s et ω_i sont les fréquences angulaires des photons de pompe, *signal* et *idler*, $\vec{k}_p$, $\vec{k}_s$ et $\vec{k}_i$ sont les vecteurs d'onde dans le cristal des photons de pompe, *signal* et *idler*. Ces équations définissent l'accord de phase.

Dans ce processus, les photons sont crées simultanément. La conversion paramétrique spontanée est dite de type I, si la polarisation des photons *signal* et *idler* est identique et or-

thogonal aux photons de pompe. Lorsque les polarisations des photons *signal* et *idler* sont orthogonales, la conversion paramétrique spontanée est dite de type II.

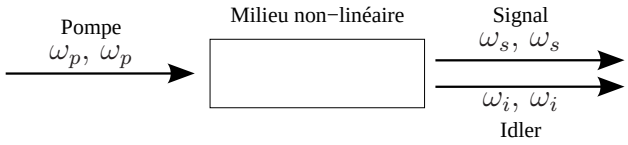


FIGURE 4.1 – *Conversion paramétrique spontanée. Un photon de pompe peut créer un photon signal et un photon idler avec conservation de l'énergie et de l'impulsion.*

4.1.2 Intrication

L'intrication ou la non séparabilité quantique est certainement la caractéristique qui différencie le plus la mécanique quantique de la mécanique classique. Deux particules intriquées n'ont pas un état individuel bien défini, mais seul l'état de la paire est défini. L'intrication est à la base du paradoxe EPR [4] et des corrélations quantiques très particulières qui en découlent.

L'intrication peut se faire sous plusieurs formes, en polarisation, en énergie-temps, ou superposition temporelle parmi d'autres degrés de liberté possibles. Nous allons étudier l'intrication de deux photons en *time-bin*. Avec une intrication en *time-bin*, les photons peuvent être présents soit à t_0, soit à $t_0 + \Delta t$, ..., soit à $t_0 + j\Delta t$. Ainsi, si un photon est mesuré dans un *time-bin* j, alors le second photon intriqué photon sera dans le même *time-bin*. Toutefois avant de faire la mesure, nous ne savons pas si les photons sont dans le *time-bin* $j-1$, j ou $j+1$. S'il y a deux temps possibles, l'intrication est d'ordre deux et les états à deux niveaux associés sont appelés *qubits*. S'il y a d temps possibles, l'intrication est d'ordre d et les états à d niveaux associés sont appelés *qudits*.

4.2 Principe de l'expérience

Tout d'abord, notons que l'intrication à hautes dimensions peut être créée de deux manières. De l'intrication à multi-photons (plus de 2) peut être crée par conversion paramétrique d'ordre élevé [54, 55, 56].

La seconde solution consiste à garder deux photons, mais à les intriquer dans un système à hautes dimensions. Cette seconde technique a l'avantage de ne nécessiter que la création et la détection de deux photons, ainsi l'efficacité est plus grande et le taux de détection plus élevé. Cela peut être obtenu de différentes manières. Par exemple, l'intrication d'ordre élevé en moment angulaire a été démontrée dans [57, 58]. Toutefois, l'intrication en *time-bin* semble plus appropriée pour obtenir facilement de l'intrication à hautes dimensions. Ceci est réalisé simplement en reprenant la même configuration que celle utilisée dans [59, 60]. Cependant, dans les expériences précédentes, l'analyse de l'intrication se faisait avec un interféromètre Michelson [61], c'est-à-dire à deux dimensions. Dans cette expérience, nous allons utiliser un interféromètre à « hautes dimensions ».

Pour réaliser un interféromètre à hautes dimensions, plusieurs possibilités s'ouvrent à nous. Nous pouvons par exemple réaliser un interféromètre Michelson à hautes-dimension, donc

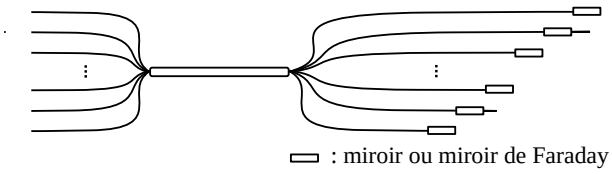


FIGURE 4.2 – *Interféromètre Michelson à hautes dimensions.*

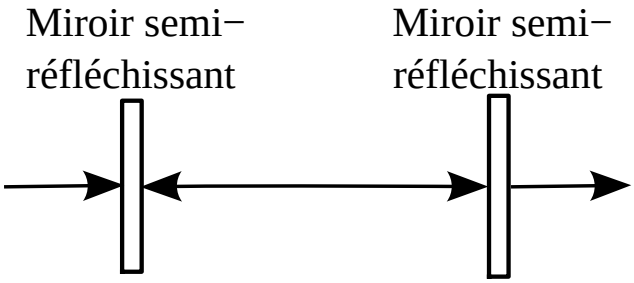


FIGURE 4.3 – *Interféromètre Fabry-Perot. La lumière peut faire de multiple aller-retour entre les deux miroirs semi-réfléchissants.*

avec plus de deux bras (FIG. 4.2). Cependant, un tel interféromètre n'est pas aisé à réaliser. Nous avons pris l'option de réaliser un interféromètre de type Fabry-Perot [61] (FIG. 4.3). Dans un tel interféromètre, les photons peuvent faire de multiples aller-retour grâce aux miroirs semi-réfléchissants avant d'en sortir. Ainsi, nous avons de multiples possibilités d'interférences, en entrant avec des photons intriqués en *time-bin*.

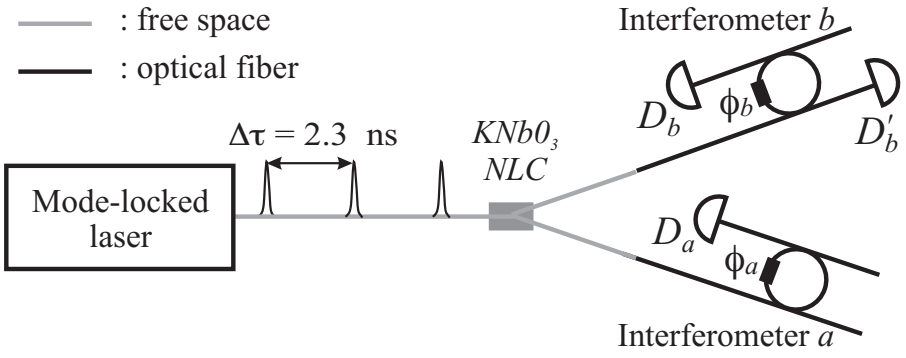


FIGURE 4.4 – *Schéma de principe simplifié.*

Sur la figure FIG. 4.4, nous pouvons voir un schéma de principe de l'expérience. Les impulsions sortant du laser *mode-locked* passent à travers un cristal non-linéaire ($KNbO_3$ NLC). Un laser *mode-locked* signifie que la relation de phase entre impulsions successives est constante. Chaque impulsion laser peut produire une paire de photons par conversion paramétrique de type I, avec une certaine probabilité. Ainsi, cela permet de créer de l'intrication à hautes dimensions en superposition temporelle en nous assurant qu'une seule paire de photons est crée dans les d impulsions définissant notre *qudit*. À la sortie du cristal, chacun des photons de la paire créée est collecté dans une fibre monomode. Les photons arrivent dans leur interféromètre respectif. Ces interféromètres de type Fabry-Perot sont réalisés de manière à ce que le temps de parcours pour un tour corresponde à $\Delta\tau = 1/f_{laser}$ où f_{laser} est la fréquence de répétition du laser. Nous avons ainsi une sorte d'interféromètre Fabry-Perot à

deux photons.

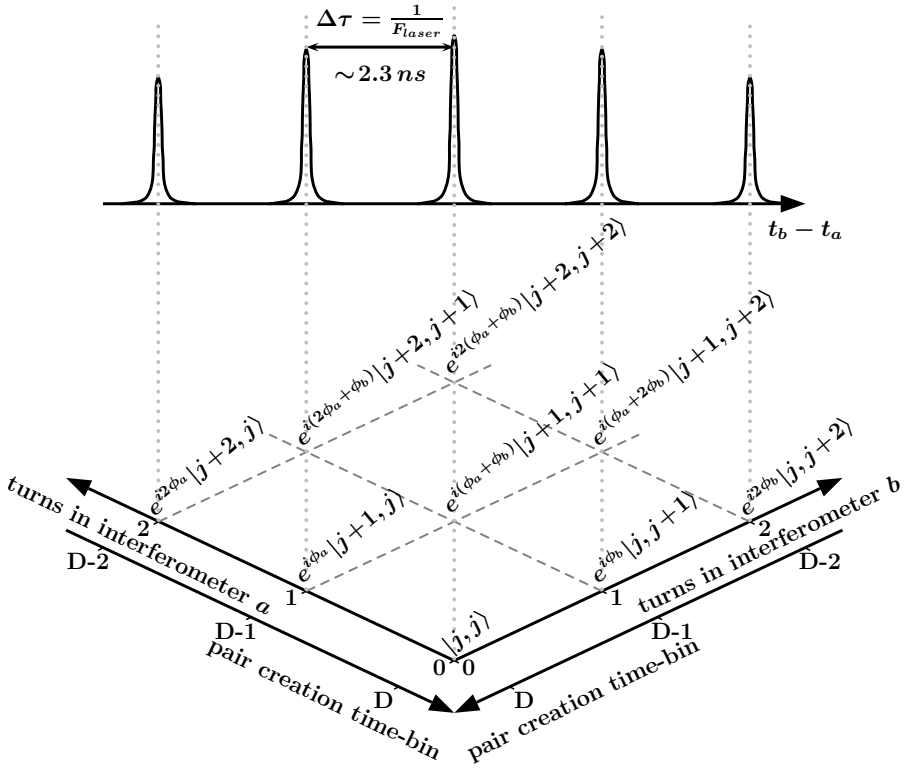


FIGURE 4.5 – *Coïncidences en fonction de la différence de temps d'arrivée sur les détecteurs D_a et D_b. Les pics correspondent à la somme des différents termes interférents pour une différence de temps donnée. Les pics sur la gauche (droite) du pic central correspondent au cas où les photons feraient plus (moins) de tours dans l'interféromètre a que dans le b.*

Pour l'expérience, nous allons mesurer les coïncidences en fonction de la différence de temps d'arrivée sur les détecteurs D_a-D_b et D_a-$D_b{}'$. Pour les détecteurs D_a et D_b le résultat attendu est présenté sur la figure FIG. 4.5.

Dans [62], la hauteur des différents pics est calculée. Nous obtenons comme probabilité de coïncidences P_n entre D_a-D_b :

$$\begin{aligned} P_{n=0} \equiv P_0 &\sim (t_{1a}t_{1b}t_{2a}t_{2b})^2 \left| \frac{1}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P_{n<0} &= (r_{2a}r_{1a})^{2|n|} P_0 \\ P_{n>0} &= (r_{2b}r_{1b})^{2n} P_0 \end{aligned} \tag{4.1}$$

où :

- par convention, $n = 0$ pour les photons parcourant le même nombre de tours. Sur la gauche (droite) du pic central, les pics sont numérotés par -1, -2, ... (1, 2, ...).
- t_{mx} et r_{mx} sont les amplitudes de transmission et de réflexion du premier ($m = 1$) et second (m=2) coupleur des interféromètres. Par convention, le photon réfléchi reste dans la même fibre.

- ϕ_a et ϕ_b sont les phases par passage dans les interféromètres a et b.

Encore deux remarques :

- pour voir les interférences à hautes dimensions, nous devons choisir $t_{mx} << r_{mx}$
- la dépendance en phase est la même pour tous les pics, alors ils oscillent de manière synchrone.

Pour la probabilité de coïncidences P'_n entre D_a-$D_b{}'$, nous obtenons :

$$\begin{aligned} P'_{n=0} \equiv P'_0 &\sim \left(\frac{t_{1a}t_{2a}}{r_{1b}}\right)^2 \left| - r_{1b}^2 + \frac{t_{1b}t_{2b}r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P'_{n<0} &= (r_{2a}r_{1a})^{2(|n|-1)} P'_0 \\ P'_{n=1} \equiv P'_1 &\sim (t_{1a}t_{2a}t_{1b}^2 r_{2b})^2 \left| \frac{1}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P'_{n>0} &= (r_{2b}r_{1b})^{2(n-1)} P'_1 \end{aligned} \tag{4.2}$$

où par convention, $n = 0$ pour les photons faisant le même nombre de tours complets. Sur la gauche (droite), les pics sont numérotés par -1, -2, ... (1, 2, ...).
Les P'_n oscillent aussi de manière synchrone. Cependant, les termes P_n et P'_n oscillent en opposition de phase. Ce comportement est logique, en supposant des pertes nulles, le nombre total de photons sortant de l'interféromètre b doit être constant par conservation de l'énergie. C'est bien ce que nous pouvons voir sur la figure FIG. 4.6. Nous voyons également que nous avons typiquement des courbes de transmission à travers un interféromètre Fabry-Perot, c'est-à-dire des interférences à chemin multiples.

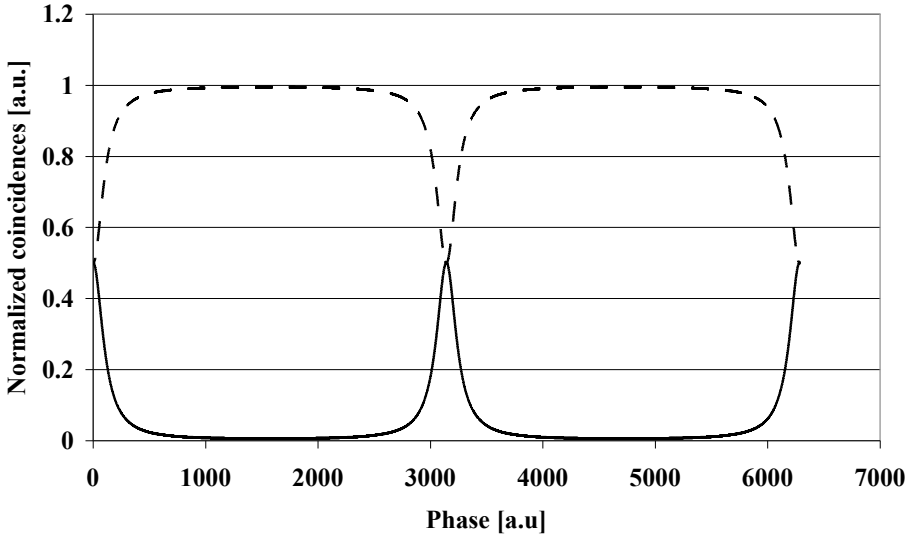


FIGURE 4.6 – *Simulation des coïncidences normalisée en fonction de la phase. La ligne pleine correspond aux coïncidences D_a-D_b et la ligne traitillée aux coïncidences D_a-D'_b. On voit que la somme des deux courbes est constante (conservation de l'énergie) (sans pertes, $r_{mx} = \sqrt{0.9}$).*

4.3 Implémentation

La figure FIG. 4.7 présente le schéma de l'expérience. Un train d'impulsion « infini » sort du laser *mode-locked*. Nous nous assurons que le laser est monochromatique à 532 nm grâce au prisme équilatéral et à l'iris.

Dans le cristal non-linéaire de niobate de potassium, des paires de photons non-dégénérés à 810 nm/1550 nm sont créées avec une probabilité de création par impulsion inférieure au pour-cent par impulsion du laser de pompe. Ainsi, nous évitons les problèmes de paires multiples qui réduisent les interférences quantiques. Le miroir dichroïque DM réfléchit les photons à 1550 nm et transmet les photons à 810 nm. Ainsi, nous pouvons optimiser le couplage des photons dans des fibres monomodes pour chaque longueur d'onde. Chaque optique de couplage comprend deux lentilles, la première pour collimater le faisceau et le second pour focaliser la lumière à l'entrée de la fibre monomode.

Pour ne pas détecter les photons de pompes, nous devons utiliser des filtres. Pour les photons à 810 nm, il y a un réflecteur à 532 nm, un filtre RG 610 et un filtre passe-bande de 10 nm de largeur totale à mi-hauteur (FWHM) et centré à 810 nm. Pour les photons à 1550 nm, il y a un filtre silicium suivi d'un filtre passe-bande de 10 nm FWHM centré à 1550 nm. Voilà, nous avons fini la description de notre source. Regardons maintenant la partie de détection de l'intrication à hautes dimensions que nous avons créée.

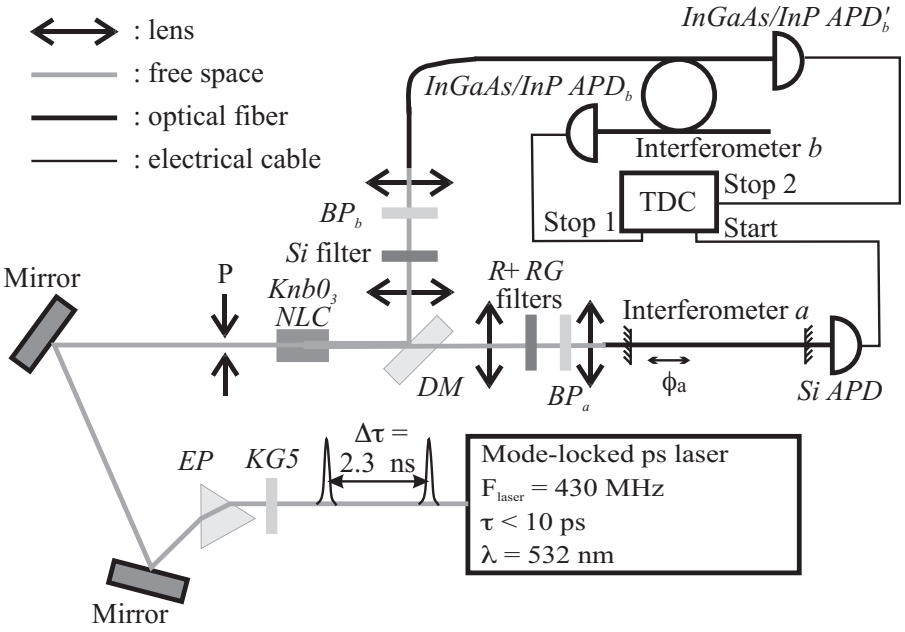


FIGURE 4.7 – *Implémentation de l'expérience d'étude de l'intrication à hautes dimensions. KG5 : filtre ; EP : prisme équilatéral ; P : iris ; $KNb0_3$ NLC : cristal non-linéaire de niobate de potassium ; BP_A et BP_B : filtres passe-bande. Pour les détails de fonctionnement, voir texte.*

L'interféromètre utilisé avec les photons à 1550 nm consiste en une boucle réalisée à l'aide de deux coupleurs R/T=90/10 (R : réflexion, T : transmission). Pour optimiser les interférences, nous plaçons un contrôleur de polarisation à l'intérieur de la boucle. Afin de faciliter l'alignement en longueur du second interféromètre avec le premier, le second est réalisé avec une simple fibre monomode à 810 nm, aux extrémités de laquelle des miroirs diélectriques

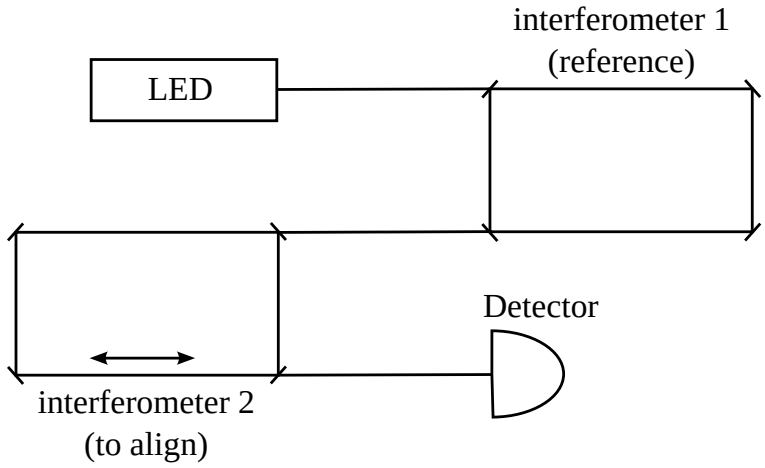


FIGURE 4.8 – *Interférence à faible cohérence.*

R/T=90/10 ont été déposés. La fibre est coupée quelques dixièmes de millimètre trop courte. Grâce à l'élasticité de la fibre, il est possible d'ajuster sa longueur avec le premier interféromètre. Pour étirer la fibre, nous utilisons un étage de translation pour l'alignement grossier. Un actuateur piézo-électrique permet l'ajustement fin.

Les photons à 810 nm sont détectés par des photodiodes avalanches silicium à comptage de photons. Les détections sur ce détecteur vont enclencher le *time-to-digital converter* et les détecteurs InGaAs/InP. Les détecteurs InGaAs/InP sont utilisés avec des portes de 50 ns de larges environ. Le *time-to-digital converter* qui enregistrent les coïncidences.

L'alignement des interféromètres est le premier point critique. En pratique, l'alignement est fait avec de l'interférométrie à faible cohérence à l'aide d'un interféromètre *bulk* additionnel. Le principe est représenté sur la figure FIG. 4.8. Nous mettons une source, les deux interféromètres à aligner en série et un système de détection. Pour l'alignement de l'interféromètre b et de l'interféromètre additionnel, nous utilisons une diode électroluminescente, comme source, et un analyseur de dispersion de mode de polarisation (PMD), comme système de détection. En fait, nous utilisons simplement le fait que l'analyseur PMD contient un interféromètre dont on peut modifier la longueur d'un bras. Si les interféromètres ont des déséquilibres de longueur différents trois pics apparaissent sur la mesure avec l'analyseur PMD. Lorsque l'alignement est correct (même différence de chemin), il ne doit y avoir plus qu'un seul pic sur l'analyseur PMD.

Pour l'alignement de l'interféromètre a avec l'interféromètre additionnel, la source est une LED et pour le détecteur, nous utilisons un détecteur silicium à photon unique. Nous changeons de détecteur, car l'analyseur PMD ne fonctionne pas à 810 nm. Nous faisons varier la longueur de l'interféromètre à aligner, lorsque les deux interféromètres sont alignés dans la longueur de cohérence de la diode, nous voyons des phénomènes d'interférences apparaître sur le détecteur.

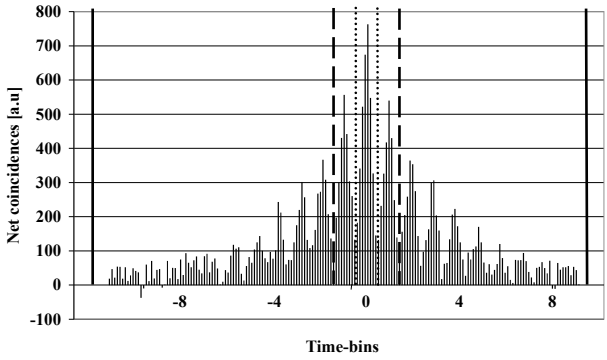
La cavité d'un laser est aussi aligné avec l'interféromètre additionnel en envoyant directement la lumière dans l'interféromètre et en regardant les fluctuations dans la puissance de détection sur le détecteur classique à la sortie.

L'alignement le plus fin doit être fait pour les deux interféromètres qui doivent être alignés dans la longueur de cohérence des paires de photons (environ 120 μm). L'alignement avec la pompe est plus facile, car la longueur de cohérence de la pompe est d'environ 2 mm dans les

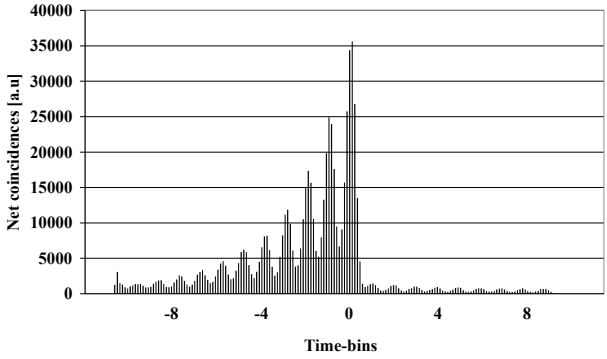
fibres.

4.4 Résultats expérimentaux

Le résultat de mesures de coïncidences accumulées entre D_a-D_b et D_a-$D_b{}'$ est présenté sur la figure FIG. 4.9. Les différentes fenêtres sur la figure FIG. 4.9(a) définies par les lignes verticales pleines, traitillées et pointillées sont utilisées pour compter les détections sur la porte entière, trois pics ou un seul pic respectivement sur la figure FIG. 4.10.



(a) Coïncidences D_a-D_b.



(b) Coïncidences D_a-D'_b.

FIGURE 4.9 – *Coïncidences nettes en fonction de la différence de temps d'arrivée. Comme $T << R$, les coïncidences accumulées en (a) sont moins importantes qu'en (b).*

La figure suivante (FIG. 4.10) présente les coïncidences entre D_a et D_b en fonction du temps, c'est-à-dire en fonction de la phase. En effet, nous changeons la tension sur l'actuateur piézo-électrique au cours du temps et donc la longueur et la phase de l'interféromètre a. Comme attendu, nous retrouvons les courbes typiques des interféromètres Fabry-Perot, signature d'interférences à hautes dimensions. Nous pouvons aussi voir que le pic central, les trois pics centraux ou l'ensemble des pics oscillent de manière synchrone, comme attendu théoriquement.

Sur la figure FIG. 4.11, nous avons les coïncidences D_a-D_b et D_a-$D_b{}'$ sur la porte entière,

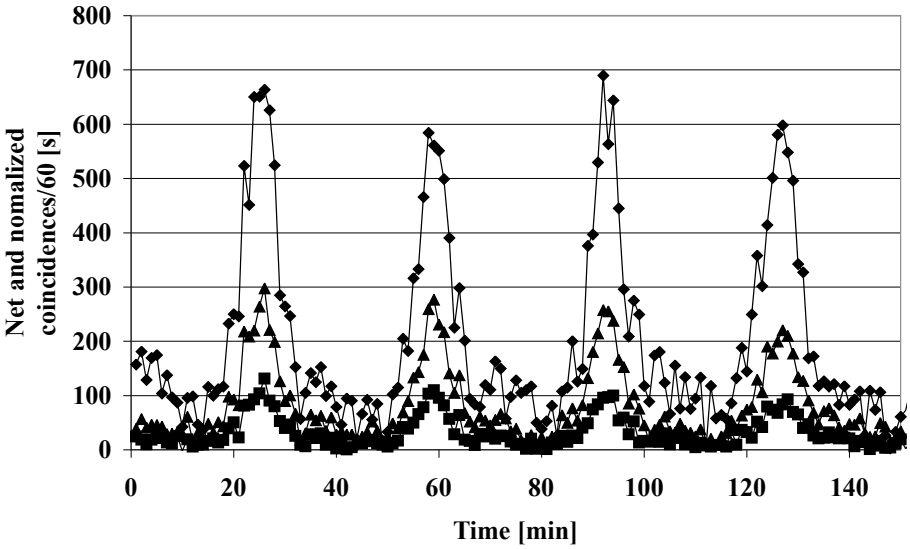


FIGURE 4.10 – *Coïncidences nettes et normalisées entre D_a et D_b. Les interférences pour le pic central (♦), les trois pics centraux (▲) et la porte entière (♦).*

et des simulations. Pour faire ces simulations, nous avons dû prendre en compte certaines limitations expérimentales :

- il y a des pertes d'environ 5 % par tour dans les interféromètres,
- la lumière n'étant pas monochromatique la phase appliquée n'est pas constante. Nous avons considérer une FWHM de 10 nm à 1550 nm correspondant à une FWHM de 5.4 nm à 810 nm,
- des petites fluctuations de température induisent une variation de la phase. Nous avons considéré des fluctuations de phase gaussiennes avec une FWHM de $\pi/8$.

Les problèmes d'alignement de polarisation n'ont pas été pris en considération dans les simulations. Cependant, nous avons essayer de limiter au maximum ce problème en alignant au mieux la polarisation dans l'interféromètre b et en essayant de minimiser la biréfringence dans l'interféromètre a [62].

Les résultats expérimentaux et théoriques sont assez proches. Les différences peuvent provenir du fait que les simulations ne prennent pas en compte l'ensemble des paramètres en jeu (polarisation ou dimension de l'intrication limitée, par exemple). Nous pouvons donc considérer que nous avons bien créé puis détecté l'intrication à hautes dimensions.

4.5 Conclusion

Avec cette expérience, nous avons pu démontrer de l'intrication ou corrélations quantiques à hautes dimensions en *time-bin*. La création de cette intrication est assez aisée à l'aide d'un laser *mode-locked* et d'un cristal non-linéaire. Cependant, son analyse est plus difficile. La réalisation des interféromètres et surtout leur alignement ne sont pas aisés.

Ainsi malgré certains avantages théoriques avec les systèmes à hautes dimensions, l'utilisation en vue d'une application proche dans des protocoles d'information quantique semble peu

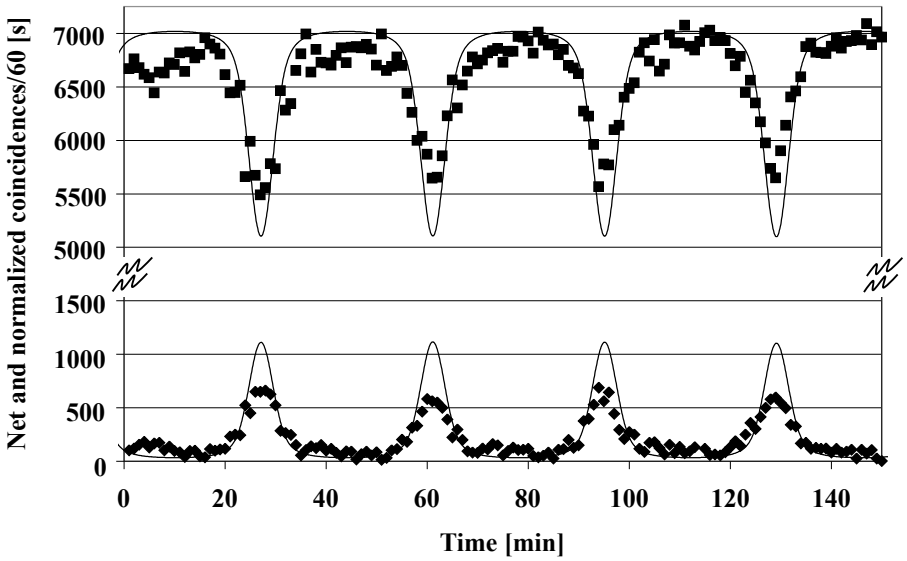


FIGURE 4.11 – *Comparaison entre les résultats expérimentaux et les simulations numériques.* ♦ *: coïncidences* D_a-D_b *;* ■ *: coïncidences* D_a-D'_b*. Voir texte pour des détails.*

probable. Les difficultés expérimentales additionnelles excèdent les avantages par rapport aux systèmes à deux niveaux.

Chapitre 5

Conclusion

Dans cette thèse, nous avons étudié différents effets découlant de la mécanique quantique. Les propriétés quantiques comme la cohérence quantique, les corrélations quantiques, la superposition quantique ou encore les perturbations induites lors de la mesure d'objets quantiques peuvent être utilisées dans le domaine de l'information quantique. L'information quantique tire avantage des propriétés quantiques, pour obtenir des résultats plus puissants qu'en information classique. Parmi les sujets venant du domaine de l'information quantique, l'un est sur le point d'atteindre le monde réel : la cryptographie quantique ou la distribution quantique de clés. Avec la distribution quantique de clés et le protocole à masque jetable, il est possible d'échanger des données de manière parfaitement sécurisée. Deux start-up proposent des systèmes commerciaux [9, 10]. Notons encore que, de nombreuses sociétés venant du monde de l'information classique s'intéressent au sujet de l'information quantique (Fujitsu, HP, IBM, Mitsubishi, NEC, Toshiba, ...). Ainsi, le domaine semble promis à un bel avenir.

Revenons sur les principaux résultats obtenus durant cette thèse de doctorat. Durant cette thèse, nous avons étudié différents problèmes dans lesquels les interférences quantiques jouent un rôle. Dans le chapitre 2, nous avons étudié le système *plug&play* pour la distribution quantique de clés, un système auto-aligné et auto-stabilisé. Cette expérience était vraiment la plus appliquée de cette thèse. Néamoins, elle utilise les propriétés fondamentales de la physique : les interférences quantiques et les perturbations induites lors de la mesure d'un état quantique inconnu. Les interférences quantiques d'impulsions cohérentes faibles permettent de générer la clé entre deux personnes distantes. La sécurité de ce système repose sur le fait, qu'à cause des perturbations induites lors de la mesure d'états quantiques (impulsion cohérentes faibles dans notre cas), les interférences quantiques disparaissent. Dans cette expérience, nous avons développé un système de distribution quantique de clés et nous l'avons testé dans un réseau de fibres optiques standards de Swisscom. Le système fonctionnant à 5 MHz a été testé sur des fibres aériennes, souterraines et sous-lacustres. Nous avons vérifié la stabilité dans les différents cas et prouvé l'auto-stabilité et auto-alignement du système. Nous avons estimé un taux de clé nette de 50 Hz sur 67 km. Le système a été repris et développé pour donner un produit complètement fonctionnel [9].

Dans le chapitre 3, nous avons proposé un nouveau protocole de distribution quantique de clés. Ce nouveau protocole doit permettre d'atteindre des taux de clé nette plus élevés. L'émetteur envoie soit des impulsions vide (0), soit des impulsions cohérentes atténuées (μ). Deux *qubits* non orthogonaux, séquences $0 - \mu$ et $\mu - 0$, sont alors encodés en superposition temporelle. La meilleure discrimination entre ces deux états correspond à une simple mesure

du temps d'arrivée ce qui permet alors de crée la clé secrète. Pour assurer la sécurité du système, la cohérence entre deux impulsions non-vide successives est vérifiée avec un interféromètre. De part sa conception, le système est résistant aux attaques de type *photon number splitting*. Pour ce protocole, cette attaque équivaut à une attaque interception-renvoi, une attaque individuelle, donc brisant la cohérence quantique entre impulsions μ successives. Dans une expérience de principe, nous avons démontré le fonctionnement du système. Après cela, nous avons développé un système permettant d'envoyer une séquence de 1 Mo d'impulsions à une fréquence de 760 Mhz (380 MHz pour les *bits* logiques). Nous avons réussi la modulation des données à l'envoi. Cependant, nous avons eu quelques problèmes avec la partie de détection. Néanmoins, nous espérons résoudre ces problèmes en développant un nouveau prototype qui devrait permettre des échanges quantiques de clés brutes dans quelques mois. L'année prochaine, pour le projet SECOQC, le système devra être complètement fonctionnel avec les processus de correction d'erreurs, d'amplification de confidentialité et d'authentification.

Finalement, dans le chapitre 4, nous avons étudié des interférences à hautes dimensions d'un point de vue plus fondamental. Dans cette expérience, nous avons créee de l'intrication à hautes dimensions en superposition temporelle ou *time-bin* grâce à un laser *mode-locked* et un cristal non-linéaire. L'analyse de l'intrication est effectuée grâce à deux interféromètres Fabry-Perot, créant ainsi un interféromètre de type Fabry-Perot à deux photons. Nous avons enregistré les coïncidences à la sortie des interféromètres et en faisant varier la phase nous avons démontré l'intrication à hautes dimensions. Cette expérience nous a permis d'observer des effets fondamentaux qui pourraient aussi être utilisés dans de nouveaux protocoles quantiques. Toutefois, une application pratique proche semble peu probable à cause de la complexité expérimentale.

Pour conclure, durant ces dernières années, de grands progrès ont été réalisés dans le domaine de l'information quantique, et nous pouvons espérer que dans les années à venir, d'autres idées émergeront dans ce domaine et permettrons encore plus d'applications de la physique fondamentale dans la vie de tous les jours.

Part II

English version

Chapter 6

Introduction

In the 19th century, firstly with Young and Fresnel, then with Maxwell with his electromagnetic theory, a modern, wave-based, theory developed allowing us to explain the phenomena of optics. Only the photoelectric effect discovered by Hertz and blackbody radiation with the ultraviolet catastrophe posed problems. In 1900 and with reluctance Planck introduced the idea that thermal radiation could only be emitted or absorbed in the form of discrete quanta which resolved the ultraviolet catastrophe [1]. In 1905, among the four revolutionary papers published by Einstein, one of them [2] formed the basis for the revolution of the quantum mechanics, the theory describing what take place at the level of particles. Taking the general idea of Planck, Einstein explained that the corpuscles or quanta of light are not only consequence of theoretical tricks, but these quanta had a physical reality. So he gave a complete explanation of the photoelectric effect and was later awarded the Nobel Prize for this in 1921. In 1924, quanta of light were directly observed for the first time by Compton effect (Nobel Prize in 1927). In 1926, a chemist named Lewis proposes the word 'photon' to describe the quanta of light.

In 1935, Einstein along with Podolsky and Rosen published a famous paper [4], describing the EPR paradox: a paradox describing the peculiar properties of quantum non-locality. This paper wanted to demonstrate that quantum mechanics didn't provide a complete description of reality. It explained that particles in special states, later called entangled states, show correlations when they are space-like separated. Systems entangled, with two or more particles, are such that the state of one or the other of the particles is not well defined, only the global state is defined until the measurement process. For example, entangled photons in polarisation are simultaneously in horizontal and vertical polarisations. Suppose the photons are carefully moved apart. When we measure one photon in one polarisation, the second one takes immediately the same one. For Einstein *et al.*, this seemed inconceivable and hence quantum mechanics was not a complete theory.

The EPR paradox, which was initially a thought experiment came closer to being a true experiment thanks to the Bell inequalities [5]. Theses inequalities are violated by quantum theory but not by classical and local theories. The EPR paradox effectively became an experimental problem thanks to the work of Freedman and Clauser [6], Fry and Thompson [7], then Aspect, Dalibard and Roger [8] among others. They violate Bell inequalities. The non-locality of quantum mechanics is demonstrated and so Einstein *et al.* appears to be wrong. However, we have to note that there are some loopholes. For example the detection loophole. It is due to the fact that, if the detection efficiency is lower than 100 %, then we could

conclude that if there is a violation of Bell inequalities, it's only for the subset of detected particles. Different loopholes have been closed, but none of the experiments have closed all loopholes simultaneously. These experiments opened a new field of quantum mechanics, quantum information.

Indeed since the middle of 1980, these new field of quantum mechanics arose. Quantum information will use the peculiar properties of quantum mechanics, like entanglement and no-cloning, in the field of information.

6.1 Quantum information

A century after the beginning of the quantum revolution introduced by Einstein, the revolution of quantum information is still in its early stages. This aims to exploit, more profoundly, the properties of quantum mechanics. At the atomic scale, the world is quite different than that of the everyday world. Among the more striking fact of relevance to quantum information, we have:

- a measurement of an unknown state can not be made without disturbing the system,
- entangled states with their peculiar properties,
- an unknown state can't be perfectly copied,
- a state can't be measured precisely and simultaneously in two non orthogonal "directions".

At first, theses properties may seem negative. However, as we will see, this can be exploited if used wisely.

Quantum information is named by analogy with classical information. Nowadays information is recorded in term of *bits* 0 and 1. To transfer data in an optical way, for example, the bits 0 and 1 are depicted by two intensities corresponding to large numbers of photons. On the other hand, on the quantum side a, information can be written in a single photon for example. This unit of quantum information is named qubit, for *quantum bit*. The properties of qubits are wider than theses of classical bits. For example, a qubit can be in the states $|0\rangle$ or $|1\rangle$, but also in superposition $|0\rangle+|1\rangle$.

For example, we can use single photons in quantum cryptography. Cryptography is the act of transmitting data between two distant people, in secret. *Quantum* cryptography denotes that the security relies on quantum mechanics. In fact, quantum cryptography is used to exchange a common and secrete key that is used by some protocols to code the information. So we should instead speak of quantum key distribution (QKD).

To exchange the key, the emitter, Alice by convention, can send a sequence of photons with the information encoded in one of its properties (polarisation, phase, ...). The receiver, Bob by convention, choses a basis of measurement and measures the photons. Alice and Bob should find some correlations between what is sent and what is received. If a eavesdropper, Eve by convention, tries to measure the photons between Alice and Bob, she can be detected. She will introduce perturbations during the measurement of unknown quantum states. To check the security of the exchange, Alice and Bob verify the correlations between what is sent and received. So with the protocol of quantum key distribution, the check on the

confidentiality of the exchanged data relies on the properties of quantum mechanics and not on mathematical complexity, like decompositions of large numbers into prime factors for example.

Quantum key distribution is the first subject of quantum information that should find a concrete application in everyday life [9, 10]. However other applications like quantum computers could flow from quantum information theory. For these, entanglement and quantum superposition are exploited. The computation power will increase, accelerating the calculation of some important classes of problems with respect current computers. Quantum computers could be used to simulate quantum systems or search prime factors of large numbers. In the last case, calculations will be achieved exponentially faster with quantum computer than with current algorithms on classical computer. So some protocols of classical cryptography could be broken with a quantum computer. However, whereas some initial experiments have been made, there is still a long way to go before we reach a fully functional system.

6.2 This thesis

In this thesis in experimental physics, we will see how quantum interferences allow us to "play" with physics. It is split into two distinct parts: the first is very applied and deals with quantum cryptography; the second is more fundamental and concern high-dimensional entanglement, dimensions higher than two. The first part allows us to see, in practical terms, how fundamental properties of physics can be used for application in everyday life. We will see how the basis for this are simple, and yet surprisingly, they take tens of years to emerge.

In chapter 7, we will see the implementation of the plug&play quantum cryptography system, an auto-aligned and auto-stabilised system, over a distance of 67 km. The monitoring of quantum interferences ensures the security of the system. The final aim of this experiment was to realise and test a "complete" system for quantum key distribution. The development of such a system required more integration than laboratory experiments for which there are not really any space constraints. After the realisation of the prototype, we tested the system on different installed standard telecom fibres. This prototype has since been taken up again and further developed and is today commercially available [9].

In the applied part of this thesis, we also study and present, in chapter 8, the implementation of a new protocol of quantum key distribution. The security of this system is based on quantum coherence and interferences. This new protocol should allow us to overcome some limitations of the plug&play system. With this new protocol, we should obtain higher secrete bit rates and its implementation should be easier. A proof-of-principle experiment will be presented. A second experiment will be presented part of the future development of this scheme.

In the last part of this thesis, presented in chapter 9, we will see an experiment of prospective. This experiment was done to study the creation and detection of high-dimensional entanglement in temporal superposition or *time-bin*. The phenomena of high-dimensional interferences present effects which are different to that with two dimensional interferences. In this last part of this thesis, we will study quantum system, at a more fundamental level, but that could also one day be used in the field of quantum information.

Chapter 7

Plug&Play quantum cryptography on 67 km

7.1 Introduction to cryptography

7.1.1 Classical cryptography

The human race has been interested in the transmission of secret data for a very long time. A history of secret codes can be found in [11]. Probably the first attempt to communicate secretly was to use the steganography (from the Greek words "*stegano*", covered, and "*graphein*", to write). With these techniques the message was hidden under a layer of wax or under the shell of a hard-boiled egg for example. One problem with this type of technique is that if the message is discovered, it is completely intelligible to the person who intercepts it.

Cryptography (from the Greek words "*kruptos*", hidden, and "*graphein*", to write) counters this weakness. In this case the meaning of a message is hidden. So if someone intercepts the message, they still have to break the code to understand the meaning of the message. The principe of cryptography is presented in the figure Fig. 7.1. On the emitter side, Alice, an algorithm allows her to encrypt a message with a key. The encoded message is sent to the receiver, Bob, on a public channel. Bob, thanks to an algorithm and an appropriate key, can find the initial message. An eavesdropper, Eve, tries to intercept the encoded message and find its meaning.

In cryptography, we have a choice to use either asymmetric or symmetric algorithms. For the asymmetric or public-key algorithms, a different key is used for the encryption and decryption. Bob takes a private and secret key, and from it, he generates a public key that is sent to Alice. Alice uses the public key to encrypt the message and sends the encoded message to Bob, who decrypts it thanks to the secret key. The security of such an algorithm relies on computational complexity thanks to the use of one-way function $f(x)$. By definition of such a function, it's easy to calculate $f(x)$ knowing x. On the other hand, it's more difficult to calculate x from $f(x)$, the time grows exponentially with the size of the input. A simple example is the next one : the multiplication $73 \times 97 = 7081$ is easy to calculate, but the opposite, the factorization of 7081 takes more time. The problem with such an algorithm is that its security is not proven, but relies only on computational complexity.

When the algorithm and the key are the same, cryptography is said to be symmetric. The

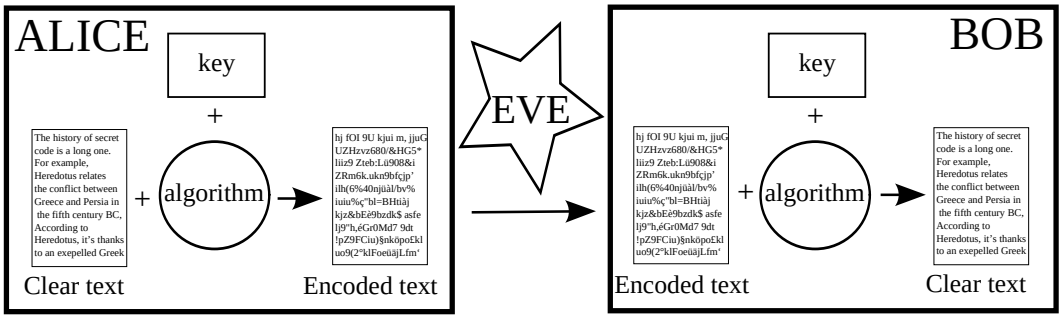


FIG. 7.1: *Cryptography. The emitter, Alice, uses an algorithm and a key to encrypt a message. The encrypted message is sent to the receiver, Bob. Bob uses an algorithm and a key to retrieve the initial message. A eavesdropper, Eve, tries to intercept the encoded message and find its meaning.*

security of theses protocols relies also on computational complexity except for one, proved secure: the one-time pad [12] (FIG. 7.2). Let's assume that the message is written in the form of binary data, the bits 0 and 1. The key used to code and decode the message needs to be a sequence of random bits of the same length as the clear text (the text to be encoded). To encrypt the message, Alice adds, bit per bit modulo 2, the message and the key. The encrypted message, a sequence of random bits without information, is sent to Bob. To find the clear text, Bob needs to add bit per bit modulo 2, the encoded message and the same key that was used by Alice to encode. If the protocol is applied properly, using a random key of the same length as the message, and importantly, only using it *one time*, then the protocol is provably secure and it's the only one.

The critical point of this protocol is the transmission of the key between Alice and Bob. Currently, the exchange of these keys is done, for example, using keys written onto CDs or DVDs. So, it is necessary to transfer the CD or DVD from Alice to Bob. It's not very practical. It's implied that Alice and Bob meet each other, or it is necessary to trust a third person. Quantum cryptography allows one to ensure the security of the key exchange.

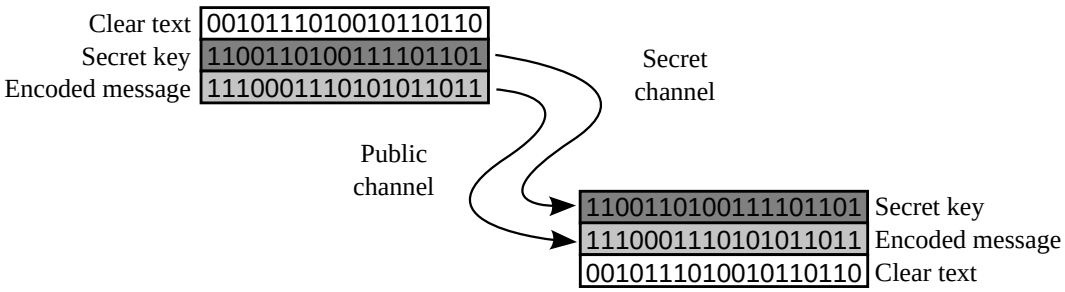


FIG. 7.2: *The One-time pad protocol. To encrypt, the message is added, bit per bit modulo 2, to a secret and random key of the same length as the message. The key has to be sent secretly to the receiver. The encoded message can be sent on a public channel. To obtain the clear message, Bob adds, bit per bit modulo 2, the secrete key and the encrypted message. This protocol is provably secure [12].*

7.1.2 Quantum cryptography

In 1984, the first paper on quantum cryptography was published by Bennett and Brassard [13], although a similar idea was presented earlier [14]. Five years later, the first experiment was performed over 32 cm in air [15]. Others protocols have been proposed by Bennett *et al.* [16] and Ekert*et al.* [17] for example. These are only few papers from a long list on the subject and for a more global perspective can be found in a recent revue on quantum cryptography by Gisin *et al.* [18]. As said before we should rather speak of quantum key distribution, because the different protocols for quantum key distribution are used to distribute a key at Alice and Bob. Then this key is used with a encryption algorithm, ideally, the one-time pad, to have a perfectly secure system. Moreover, if we have some doubt on the security during the key exchange (see below), no information is lost, because the key contains no information.

As for classical information, photons can be used for the exchange of quantum keys between Alice and Bob. However, in this case we use individual photons. The information is encoded on one of the properties of the photons, for example, the polarization, the phase or the time. By analogy with classical information, these states are called qubits for quantum bits. The security relies on the fact that an eavesdropper can't copy the quantum state of the photons (no-cloning theorem [19, 20]), nor can she measure these quantum states without disturbing them.

To understand this, let's look at the BB84 cryptographic protocol proposed by Bennett and Brassard [13]. This protocol uses four quantum states forming two maximally conjugate bases. For example, the qubits are encoded on the polarization of the photons: horizontal (H), vertical (V), for one basis; and +45 ° (+) or -45 ° (-), for the other. The value 0 is associated to polarization H and +, the value 1 to V and -. Alice sends a sequence of photons, randomly choosing the polarization for each one. Bob then measures the photons. When the basis of measurement is compatible with the sent state (base H/V with photon H or V, for example) Tab. 7.1, then the result is deterministic, otherwise, it is random. At this moment, Alice and Bob share a raw key. By comparing the basis of the measurement and the preparation, Alice and Bob can generate what is called a sifted key from the compatible cases.

Base Alice	State Alice	Logical bit Alice	Base Bob	Measure Bob	Logical bit Bob
H/V	H	0	H/V	H	0
H/V	H	0	+/-	?	?
H/V	V	1	H/V	V	1
H/V	V	1	+/-	?	?
+/-	+	0	+/-	+	0
+/-	+	0	H/V	?	?
+/-	-	1	+/-	-	1
+/-	-	1	H/V	?	?

Table 7.1: *BB84 protocol in polarization. Photons with horizontal (H), vertical (V), +45° (+) or -45° (-)polarization are randomly chosen and sent. {H,+} code 0 and {V,-} code 1. The two basis are {H/V} and {+/-}. For compatible basis, the result is deterministic (1 or 0), while for incompatible basis, it is random (?).*

To obtain the key, classically, an eavesdropper, Eve, could simply copy the information that is sent. On the quantum side, it's not possible to obtain a perfect copy, with probability 1, according to the no-cloning theorem [19, 20]. Only imperfect copies are possible and/or with probability lower than 1, see [21], or [22] for a revue. So with such an attack, Eve can obtain only partial information.

Let's see what happens with a very simple attack: *the intercept-resend*. Eve is somewhere between Alice and Bob. She makes the same type of measurement as Bob, she measures the photons in one of the two basis, and she resends photons with a polarization corresponding to her results. When Eve measures in a compatible basis with the state of Alice (50 % of the case), she obtains all information and the photon, that she sends to Bob, has the correct polarization. But, if she takes the incompatible basis, the result is random and the measured polarization makes an angle of $\pm 45^\circ$ compared to Alice's photon. In this case, she sends different states to those that Alice prepared. If Bob uses a compatible base with the initial photon of Alice, then he will have error in 50 % of the case. The total quantum bit error rate (QBER) between the sifted key of Alice and Bob is of $0.5 \times 0.5 = 25\,\%$. By monitoring the QBER in the expected correlations, Alice and Bob can make sure that the confidentiality is guaranteed. If the QBER is too large, the key is rejected, but no information is lost, because the key is only a random sequence without information.

In reality, even without an eavesdropper, there is some error in the sifted key because of experimental imperfections. Whatever the cause of the errors, they have to be removed by a classical procedure of error correction. Alice and Bob share then the same key. However, it's possible that Eve has obtained some information, either by directly attacking the quantum information exchange, or during the process of error correction, which involves further classical communication. So Alice and Bob apply another classical procedure: privacy amplification. This procedure ensures that Eve's information is lowered to an arbitrarily low level. Finally, it's necessary that Alice and Bob authenticate one another.

It is important to note that under some given conditions, essentially an bound on the QBER and known losses between Alice and Bob it's possible to obtain a secret key between Alice and Bob [23, 24]. So, by combining quantum key distribution and the one time-pad protocol, it's possible to exchange information between two distant people in a perfectly secure way.

7.2 Introduction plug&play

This work is the continuation of several experiments [25, 26, 27]. The aim was the development and testing of a prototype of quantum key distribution. In this instance, a prototype is defined to be a system that integrates the components in 19 inches racks/boxes and is transportable and ready for use in a telecom network. The developed system realizes the raw key exchange, that is, it doesn't perform the reconciliation process (error correction, privacy amplification and authentication). Nevertheless this system has been taken up again and developed by id Quantique and is today commercially available [9]. Another company has developed a similar system [10].

The principle of the plug&play system allows one to work with faint attenuated laser pulses, so we don't send single photon as previously discussed. Therefore, our pulses are characterized by a Poissonian distribution with a mean photon number μ. However, it is possible to exchange secret key under some assumptions [28, 29, 30].

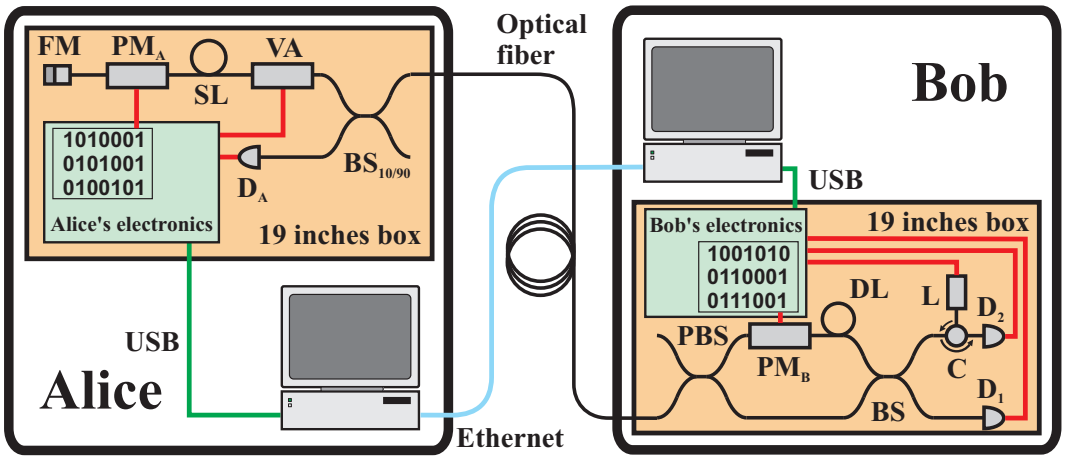


FIG. 7.3: *Implementation of the plug&play system. L : laser; C : circulator; BS : coupler; DL : delay line; PM : phase modulator; PBS : polarizing beamsplitter; D_1 et D_2 : InGaAs/InP avalanche photodiode; D_A : pre-amplified photodiode; VA : variable attenuator; SL : storage line; FM : Faraday mirror. For a more detailed explanation, see text.*

The principle scheme of the plug&play system is depicted in figure FIG. 7.3. Bob sends intense laser pulses, onto the beamsplitter BS where half of the light goes through the short arm and the rest of the light goes through the long arm of the interferometer and it's polarization is rotated by 90°. The second pulse is smaller than the first one because of the losses in the phase modulator of the long arm. The pulses of light are sent to Alice, where they are reflected and then attenuated, in order to reduce the mean number of photon of the second pulse to $\mu/2$. The second pulse is also modulated with a phase 0, $\pi/2$, π or $3\pi/2$, by the phase modulator PM_A, which is synchronized with the detector D_A.

When the photon comes back to Bob the first pulse is sent through the long arm and second pulse through the short arm. This is due to the fact that, with Faraday mirror, when light come back, its polarization is orthogonal to the original one and hence, the pulses are sent through the opposite paths, by the polarization beamsplitter, on their return. Bob choses the basis of measurement by applying a phase of 0 or $\pi/2$ on the first pulse. As a function of the phase applied by Alice and Bob, the detections are either deterministic (compatible base) or random (incompatible base) on the avalanche photodiodes (APD) D_0 or D_1.

A problem with the plug&play system is the Rayleigh backscattering. To avoid this problem, the pulses are sent in the form of a train, which arriving at Alice fills the storage line SL located after the variable attenuator. Bob opens his detectors when the train comes back. Then he sends a new train of pulses.

The main advantages of such a system is that it is auto-aligned (only one interferometer) and auto-stabilized (thanks to the Faraday mirror).

7.3 Implementation of the system

Compared to the experiment [27], some improvements have been made:

- polarizing maintaining fibers are used on Bob side, so we don't need anymore polarization controller to take full advantage of the configuration with Faraday mirror and

polarizing beam splitter.

- the system works at 1550 nm to reduce the losses in the fibers (1310 nm in the previous experiment)
- the system works at $\nu = 5\,\text{MHz}$, 2.5 MHz previously
- a dedicated electronics with programmable logic (FPGA) has been developed to control the system
- the software part has been developed for the control of the system and the exchange of the key. The communication between the hardware and the computer is done with USB links. This part of the software has been developed by Ellisys [31].

The remainder of the system is quite similar. Bob uses InGaAs/InP avalanche photodiodes in Geiger mode for the detection. To reduce the noise the detector are used in gated mode, i.e. the polarization voltage excess the breakdown voltage only for short period. We also use some dead time after a detection to avoid afterpulse [32, 33]. The detection efficiency η_B is approximately 10 % and the probability of noise is around 10^{-5} per 2.5 ns detection gate.

To avoid the Rayleigh backscattering, we send pulse-trains of 480 pulses at a frequency of $\nu = 5\,\text{MHz}$. In this way we don't exceed the capacity of the storage line SL of length $l_{SL} = 10\,\text{km}$.

7.4 Key parameters

The most important parameters for the system are calculated in [34]. The raw key rate R_{raw} is given by:

$$R_{raw} = q\nu\mu t_{AB} t_B \eta_B \eta_{duty} \eta_\tau \tag{7.1}$$

where:

- q depends on the protocol (0.5 for BB84 for example, because of incompatible bases)
- t_{AB} transmission from Alice to Bob
- t_B transmission on Bobś side
- $\eta_{duty} = \frac{l_D}{l_{AB}+l_D}$ is the factor due to the operation per train of pulses with a storage line (l_{AB}: distance Alice-Bob)
- $\eta_\tau = \frac{1}{1+\nu p_{det}\tau}$ is used to take into account the dead time on the detectors (fixed at 4 μs in the experiment) (p_{det}: probability of detection)

The QBER is defined by:

$$QBER = \frac{false\,counts}{total\,counts} = QBER_{opt} + QBER_{dark} + QBER_{after} + QBER_{stray} \tag{7.2}$$

where:

- $QBER_{opt}$ is due to misalignment of the polarization on Bob side and the stability link

- $QBER_{dark} \cong \frac{p_{dark}}{\mu t_{AB} t_B \eta_B}$ is the probability of dark count per gate p_{dark} divided by the detection probability
- $QBER_{after} \cong \sum_{n=0}^{n=\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{\nu}\right)$ is the sum of afterpulse probability between two detections ($p_{after}(t)$: probability of afterpulse per detection gate a time t after a first detection)
- $QBER_{stray}$ is due to the stray light, essentially the Rayleigh backscattering, for the plug&play configuration. However, by using the storage line, this can be avoided.

The visibility is also an important parameter and can be written as a function of the detection rates R_{right} and R_{false}, the correct and false detections rate, respectively:

$$V = \frac{R_{correct} - R_{false}}{R_{correct} + R_{false}} \tag{7.3}$$

such that we can write the relationship for the $QBER_{opt}$:

$$QBER_{opt} = \frac{1 - V}{2} \tag{7.4}$$

The last important parameter is the net key rate R_{net}:

$$R_{net} = \eta_{dist} R_{raw} \cong (I_{AB} - I_{AE}) \frac{I'_{AB}}{I_{AB}} R_{raw} \tag{7.5}$$

where I_{AB} and I_{AE} is the mutual information for Alice-Bob, and Alice-Eve, respectively, I'_{AB} is the mutual information for Alice-Bob after error correction. The evaluation of this different informations can be found in [34].

7.5 Experimental results

The system was tested on installed standard fibers in the Swisscom network. Measurement have been made on terrestrial, under lake, and aerial fibers from 8.7 to 67.1 km. Measurements of visibility are presented in Tab. 7.2. The visibility is always larger than 99 %, so according to (7.4) the optical QBER is smaller than 0.5 %. So the possible perturbation of the polarization, due to wind for aerial fiber or to vibrations for terrestrial fiber along the road, does not perturb the system. The auto-alignment works in all cases.

On the same fiber we performed a key exchange and the results can be found in Tab. 7.3. We obtain a raw key rate of 0.15 to 6.3 kHz. The QBER is between 2.0 and 6.1 %. We also calculate the net rate. Like in [35], we takes the following assumptions for Eve's capacities:

- no measure of photon number without perturbation,
- no quantum memory,
- QBER in statistical limits of estimation according to (7.2).

We estimate the net key rate between 44 Hz and 4.34 kHz.

fibre	length [km]	loss [dB]	Visibility [%]
Geneva-Nyon (under lake)	22.0	4.8	99.70 ± 0.03
Geneva-Nyon (terrestrial)	22.6	7.4	99.81 ± 0.03
Nyon-Lausanne (terrestrial)	37.8	10.6	99.63 ± 0.05
Geneva-Lausanne (under lake) A	67.1	14.4	99.62 ± 0.06
Geneva-Lausanne (under lake) B	67.1	14.3	99.66 ± 0.05
Ste Croix (aerial) A	8.7*	3.8	99.70 ± 0.01
Ste Croix (aerial) B	23.7*	7.2	99.71 ± 0.01

Table 7.2: *Results of visibility for different configuration. *The effective aerial part is 2×2.5*km. *The difference between the experiment is due to an additional 15*km *spool of fiber adds between the two segments of aerial fiber.*

7.6 Conclusion

We have shown the exchange of qubits over a distance greater than 67 km with a net estimated key rate of 50 Hz.

As previously discussed, this prototype has been used as a basis for the development of, what is now, a commercial product. It is striking to see how fundamental and simple properties of physics can be used at a very applied level. What is still more surprising is that it took so long for that the idea of quantum cryptography emerge, while now, an undergraduate student in physics can understand the basic principles, even after their first quantum mechanics lesson.

fibre	length [km]	Key [kbit]	$R_{raw}[kHz]$	QBER [%]	$R_{net}[kHz]$
Geneva-Nyon (under lake)	22.0	27.9	2.06	2.0±0.1	1.51
Geneva-Nyon (terrestrial)	22.6	27.5	2.02	2.1±0.1	1.39
Nyon-Lausanne (terrestrial)	37.8	25.1	0.50	3.9±0.2	0.26
Geneva-Lausanne (under lake) A	67.1	12.9	0.15	6.1±0.4	0.044
Geneva-Lausanne (under lake) B	67.1	12.9	0.16	5.6±0.3	0.051
Ste Croix (aerial) A	8.7	63.8	6.29	3.0±0.1	4.34
Ste Croix (aerial) B	23.7	117.6	2.32	3.0±0.1	1.57

Table 7.3: *Results of quantum key distribution for different configuration with $\mu = 0.2$. The net key rate is calculated with the raw key rate R_{raw}, the QBER and the formula (2.5).*

Chapter 8

Fast and simple quantum cryptography

8.1 Introduction

In chapter 7, we studied a quantum key distribution system that has gone on, after some additional development, to become a commercial product [9]. Despite some of its advantages, this system still has some weaknesses. Firstly, the pulses going from Bob to Alice and back and the necessity to send discrete pulse-trains, limits the maximum bit rate. From a system complexity point of view, the plug&play needs a rather large number of components. It is also necessary to actively choose, on Alice's and Bob's sides, the states and bases respectively. With this in mind we looked to develop a protocol which is easier to implement from a practical point of view. This protocol has to fulfill the following conditions:

- the system must be easy to implement with standard telecom components,
- the security must rely on quantum mechanics, like quantum coherence.

We have developed a new protocol which satisfies theses properties: the Coherent One Way (COW) protocol. It works with weak coherent pulses at 1550 nm, pulses only need to be sent one-way and the encoding of logical bits is done in time. At Bob's input, the photons can take one of two paths. On the *data line*, a simple time-of-arrival measurement allows one to generate the key. The *monitoring line*, which incorporates an interferometer, allows one to detect for the presence of an eavesdropper. We note that the data line is quite similar in [36].

8.2 Protocol

Figure Fig. 8.1 shows a schematic of the new protocol. With a CW laser followed by a intensity modulator Alice sends a sequence pulses. The pulses are either empty (0-pulse), or have a mean photon number $\mu < 1$ with a Poissonian distribution (μ-pulse) Fig. 8.2. The sequence $\mu-0$ (or $|\mu\rangle\otimes|0\rangle$) codes a logical 0, and $0-\mu$ (or $|0\rangle\otimes|\mu\rangle$) codes a logical 1. We note that, because of the vacuum component of the μ pulses, the two states are not orthogonal. Alice needs to send $\mu - \mu$ (or $|\mu\rangle \otimes |\mu\rangle$) sequences for security reasons (see below). These

sequences are named decoy sequences with reference to the *decoy states* introduce in [28, 30]. However, contrary to the decoy states, the decoy sequences don't encode logical values.

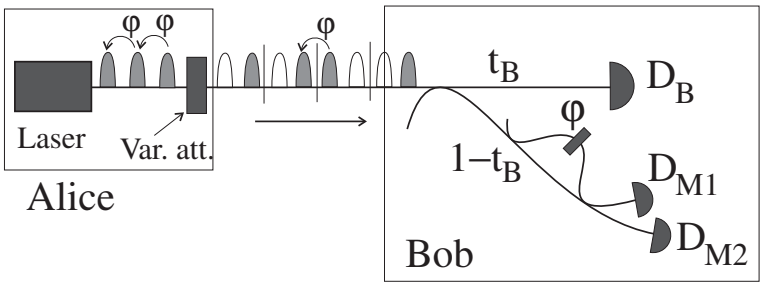


FIG. 8.1: *COW protocol. The detector* D_B *allows one to generate the key. The detectors* D_{M_1} *and* D_{M_2} *are used to check the coherence between successive* μ*-pulse and hence check the security.*

On Bob's side *data line* (detector D_B), Bob records the time-of-arrival of the photon to generate the key. This very simple measurement is the best strategy to discriminate between the two non-orthogonal states [37]. The *monitoring line*, with an interferometer and detectors D_{M_1} and D_{M_2}, allows to check the presence of an eavesdropper by checking the coherence between successive μ pulses. For example, the alignment of the interferometer can be done to have constructive interferences on D_{M_1} and destructive on D_{M_2} without eavesdropper. If an eavesdropper is present, this will change.

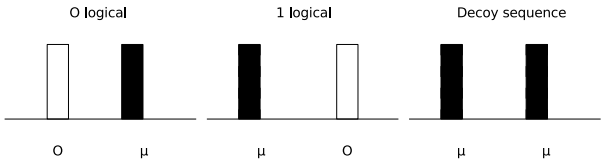


FIG. 8.2: *Bits coding for the new protocol. For each sequence the first pulse is the right one. In addition to the 0 and 1 logical bits, decoy sequence are sent for security reason (see text).*

In summary, the protocol works in the following way:

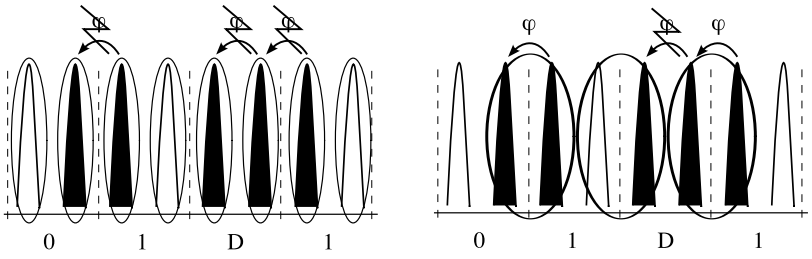
- Alice sends a long sequence of random bits, 0 and 1, with probability $(1-f)/2$ for each of them, as well as decoy sequences with a probability $f << 1$
- Bob gives the *position* (which bit window) of the bit detected by D_B and the *time* of the detection for the monitoring detectors D_{M_1} and D_{M_2}
- Alice says which detections correspond to decoy sequences and have to be removed from the results for D_B (sifting)
- Alice estimates Eve's information, from the visibility on the interferometer
- Finally, Alice and Bob perform classical process of error correction, privacy amplification and authentication.

8.2.1 Eve's attack

In [37], a first study of the security has been made, so here we will only make a brief summary. Eve can perform a *beam-splitting attack* by removing a fraction $1-t$ of the photons and transmits the rest to Bob on a lossless fiber. Of the fraction $1-t$, Eve simply measures the time of detection, because it's the better strategy to discriminate the two qubits. So, Eve can obtain the fraction $\mu(1-t)$ of the key, which we have to take into account during the privacy amplification process.

With the BB84 protocol and a lot of others ones, because of the multi-photons pulses and losses in the channel Alice-Bob, Eve can obtains information without introduce errors. These are the photon number splitting attack (PNS) [38, 39]. This attack is done individually on each pulse. Eve counts the number of photons per pulses, takes one if there is more than one photon and lets the other ones go to Bob. With this new protocol such an attack, such an individual attack breaks the coherence between successive μ pulses and induce errors (Fig. 8.3(a)). Note that in fact for this protocol, this attack is equivalent to a intercept-resend attack.

Eve could try another attack for which she makes coherent measurement of a number n of photons on two successive pulses. Let's assume that Eve is synchronized with Alice et makes this attack on the separation of two logical bits. In this case, she doesn't break the coherence for logical sequence 10 and obtains some information during the sifting process, if she measures $n > 0$. However, with the decoy sequence, she will break the coherence and then be detected (Fig. 8.3(b)).



(a) Individual attack. (b) Coherent attack.

Fig. 8.3: *Breaking of coherence. The attacks are depicted with ovals. (a) With individual attacks, the coherence is broken for all successive μ pulses. (b) For coherent attacks on two pulses, Eve is not detected except if there is a decoy sequence.*

8.3 Implementation

8.3.1 Principle experiment

The proof-of-principle was first shown in an experiment [40] where the same logical sequence, D010 (D for decoy sequence), of eight bits were repeatedly sent. The data was recorded using a time-to-digital converter (TDC) (Fig. 8.4) and the results analyzed statistically.

To generate the sequence, we developed an specific electronics. We used what is called a serializer. That allows us to separate the high speed part, with data in series, and the rest of the system working at a lower speed with data in parallel. In details, a serializer takes n bits in parallel at the input at a frequency F/n, and a clock at frequency F. At the output, the bits are sent one after the other at the frequency F.

The clock C_1 at F=434 MHz defines the time τ between two pulses in the train. So the bit frequency is 217 MHz (neglecting the decoy sequence). The clock C_2 defines the repetition frequency of 600 kHz for the sequence of 8 bits. The signal at the output of the serializer goes through a pre-amplifier, an amplifier which goes on the intensity modulator IM and so, modulates the 1550 nm CW laser according to the 8-bits sequence. The attenuation is adjusted with the variable attenuator VA to a level of 0.5 photon per μ pulse. With the same attenuator, we added 5 dB of additional attenuation to simulate 20 km of fiber losses (at 0.25 dB/km). The synchronization signal is sent via a coaxial cable from Alice to Bob.

On Bob's side, the synchronization signal is used to start the TDC and to apply 20 ns gates on the detectors D_B and D_M. With large gate times on the detectors we can register the sequence of 8 bits, but there is at most one detection per detector and per sequence because of the dead time of the detectors. The monitoring interferometer is made with a 50/50 coupler and two Faraday mirrors. Thus it is automatically aligned in polarization. We only use one monitoring detector D_M. To check the visibility, we simply change the phase in the interferometer by changing the temperature.

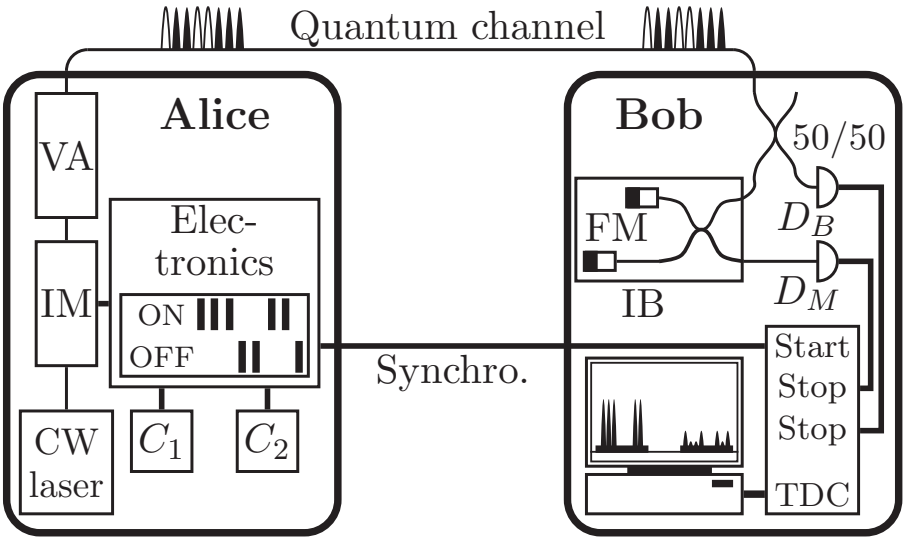


FIG. 8.4: *Proof of principle experiment.* C_1 *: pulse clock;* C_2 *: sequence clock; IM : intensity modulator; VA : variable attenuator; FM : Faraday mirror; IB : isolated box;* D_B *and* D_M *:InGaAs/InP detectors; TDC : time-to-digital converter. See text for more details.*

On D_B, the raw detection rate is 17±0.1 kHz, for a detection efficiency of 10 % and a noise probability of 2.5×10^{-5} per ns.

On D_B, the QBER is 5.2±0.4 %, 4 % of this is related to the detector and the rest is due to imperfect modulation of the pulses. On D_M, the measured raw visibility is 92 % and the net value, where we take account of the detector's dark counts and afterpulses, is 98 %.

Conclusion of first experiment

With this first experiment, we demonstrate the feasibility of the new protocol. Some improvement could be done. The detection rate, and then the key rate, could be increased by increasing the duty cycle of the system (by sending continuously 0 or μ pulses), optimizing f and t_B. It's what we have done.

8.3.2 Second experiment

After the first experiment, we developed a second system. This time, Alice can send a sequence of 1 MB of pulses, or 0.5 MB of logical bits (neglecting decoy sequences). This data is loaded from a PC to Alice's memory M via a serial port. Alice then repeatedly sends this sequence. The data transmission is performed using a programmable logic (CPLD). Alice reads the data in the memory M with a bus width of 16 bits at a frequency of 760/16=47.5 MHz. This data are sent to two 8-bit serializers S in series. At the output of the serializers, we have the sequence of pulses at 760 MHz, so that the frequency of logical bits is around 380 MHz. The outgoing pulses are amplified and go on the intensity modulator IM to modulate the CW laser. The mean intensity of the μ pulses is adjusted with the variable attenuator VA. The synchronization signal is sent from Alice to Bob on a second optical fiber with standard telecom SFP transceiver modules. The synchronization signal corresponds simply to the 760 MHz clock for which Alice removes one pulse. Bob detects the missing pulse and generates a reset signal for the 14 bits counter, 8 bits external (C) and 6 bits internal to the CPLD.

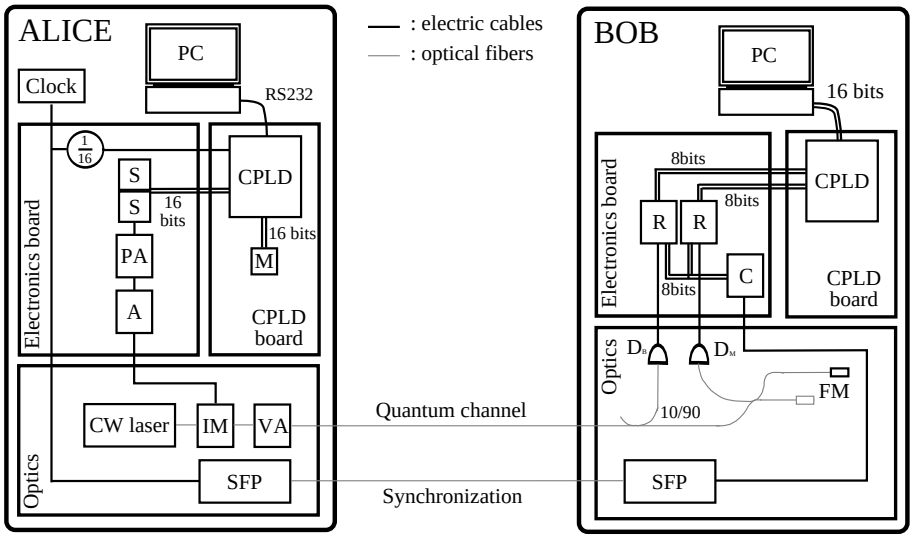


FIG. 8.5: *Second experiment. M: 1* MB *of memory; CPLD: programmable logic; S: serializer; PA: pre-amplifier; A: amplifier; IM: intensity modulator; VA: variable attenuator; SFP: transceiver module; FM: Faraday mirror; C: 8-bits counter working at 760* MHz*; R: register. For details, see text.*

The 8-bit counter works at 760 MHz and allows us to obtain the exact clock timing for of a detection and thus the logical bit. The 6-bit counter counts the overflows of the 8-bit counter. When there is a detection the value of the external counter C is put in an intermediate register

R, one for each detector, and then transferred to a programmable circuit (CPLD), and finally transferred to a PC through an acquisition card with 32 TTL digital inputs. In fact, for each acquisition, we register the 14 bits of the total counter and on bit for each detector to know which clicks. So we register 16 bits per acquisition. Overflows of the total counter (8 external + 6 internal bits to the CPLD) are also transmitted to the computer to obtain the absolute time for the detections.

To control the system, we developed a program for Alice, which allows us send data stored in the memory or pre-defined sequences. On Bob's side, we developed a small program to register the data. Unfortunately, the results of this experiment were not entirely conclusive. Alice's part works well and we can put data in the memory and use this sequence to modulate the CW laser. We tested different sequences and check the modulation on an oscilloscope. On Bob's side there is a problem with the acquisition of data. Sometimes, generally less than in 1 % of the detections, the time of the detection $n + 1$ is smaller than the time of the detection n. Unfortunately, we have not resolved this problem though it is hoped it will be overcome in the process of developing a more complete system that is currently being developed for the SECOQC project [41].

8.3.3 Future developments

For the european project SECOQC we have to realize a system working 24 hours a day and seven days a week in a telecommunication network. This protocol is one of several different approaches being developed for this project. For this, we will use a more powerful programmable logic (FPGA rather than CPLD). By doing this we can use the internal serializer in the FPGA, which will simplify the construction of the system, the adjustment of the delays between the different signals and hopefully resolve the previously mentioned timing problem. Alice and Bob's systems will be integrated into 19 inches racks/boxes. The software part for the automatization of the system should be developed and runs on a Linux system. The system will have to allow quantum key distribution with the complete classical process, error correction, privacy amplification and authentication.

The poor performances is a problem with the current detectors at 1550 nm, particularly when the speed of the system is high. The current InGaAs/InP detectors can not exceed a detection rate higher than 100 kHz, because of the detector dead time of 10 μs, that is used to avoid afterpulses. Moreover, the jitter can become a problem with increasing speed. However, there are some possible solutions that are emerging. Firstly there is new InGaAs/InP detectors [42, 43], which promise to have better characteristics, but these still have to be tested.

Alternatively we can use up-conversion detection, it is possible to reach detection rates of few MHz [44, 45]. However, if we want to use commercial products, the construction of these detectors has to be improved. Finally, we could consider superconductor detectors. In this case, we could expect detection rates of a few GHz [46, 47], but at cryogenic temperatures and then this becomes less realistic for an application.

If this problem of detection is resolved, the classical process of reconciliation will be a more important problem. More precisely, the error correction will become critical. So it will be necessary to optimize this phase to avoid this bottleneck.

A last problem is the generation of random data to modulate the laser. We need a true random number generator and not a pseudo-random generator to have a complete security.

8.4 Conclusion

The new quantum cryptographic protocol has been implemented in a first proof-of-principle experiment. For the first experiment, the results were conclusive. For the second experiment, the results were less conclusive. Nonetheless, we sent logical bits at a frequency of 380 MHz and we partially succeeded in data acquisition. Despite this, it has allowed us to make some preliminary experiments with rapid electronics and highlighted some of the problems that we will need to overcome for future developments.

With this experience, and of course some additional development, we should be able to obtain a fully functional system at a frequency of some hundred of MHz in the next year and in the near future, at few GHz.

Chapter 9

High-dimensional entanglement

9.1 Introduction

In contrast to the previous experiments, this chapter deals with a subject of a more fundamental nature. This experiment is approached more from a quantum *optics* perspective. However, high-dimensional entanglement could be used for experiments more oriented towards quantum *information*. For example, quantum key distribution is tolerant to higher noise for higher dimensions [48]. It's also possible to reduce the required detection efficiency to close the detection loophole in the EPR paradox [49]. High-dimensional systems allows a larger violation of local realism [50] and with a higher robustness to noise [51].

Let's start with the introduction of spontaneous parametric down-conversion and entanglement.

9.1.1 Spontaneous parametric down-conversion

The figure Fig. 9.1 represents the non-linear effect of spontaneous parametric down-conversion (SPDC) [52, 53]. At the input of the crystal, we have a pump photon (ω_p, k_p) and at the output, we have a signal photon (ω_s, k_s) and an idler photon (ω_i, k_i). Non-linear effects are due to high order term of the susceptibility, the second order term $\chi^{(2)}$ in our case. To obtain non-linear effect, we have to carefully choose the laser and the crystal and the orientation of its optical axis in relation with laser polarization. We must obey energy and momentum conservation :

$$\hbar\omega_p = \hbar\omega_s + \hbar\omega_i$$
$$\hbar\vec{k_p} = \hbar\vec{k_s} + \hbar\vec{k_i}$$

where ω_p, ω_s and ω_i are the angular frequency of the pump, signal and idler respectively, $\vec{k_p}$, $\vec{k_s}$ and $\vec{k_i}$ are the wave vector in crystal of the pump, signal and idler photons respectively. These equations define the phase matching.

In this process, the signal and idler photons are created simultaneously. The spontaneous parametric down-conversion is said to be of type I, when the signal and the idler photons have the same polarization and are orthogonally polarized to the pump photons. When the

polarizations of the signal and idler photons are orthogonal, the spontaneous parametric down-conversion is said to be of type II.

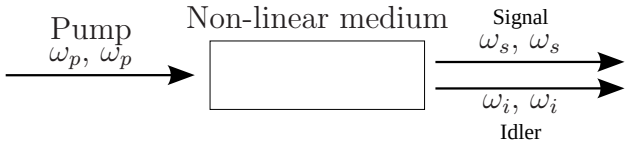


FIG. 9.1: *Spontaneous parametric down-conversion. A pump photon creates a signal and an idler photon with energy and momentum conservations.*

9.1.2 Entanglement

Entanglement is one, if not the, characteristic which differentiates quantum mechanics from classical mechanics. Two entangled particles do not have a well defined individual state. Only the state of the pair is well defined. The entanglement is at the heart of the EPR paradox [4] and of the peculiar quantum correlations.

Entanglement can be realized in polarization, in energy-time or in time-bin amongst others possible degrees of freedom. We will study time-bin entanglement of two photons. With entanglement in time-bin, the photon pair can be present at one of the times t_0, $t_0 + \Delta t$, ..., $t_0 + j\Delta t$, ... Then if one photon is in the time-bin j, the second entangled photon will also be in the same time-bin. However before the measurement, we don't know if these are in the time-bin $j-1$, j or $j+1$. If there are two possibles times, the entanglement is of order two and the associated 2-levels states are named qubits. If there are d possible time-bin, the entanglement is of order d and the associated d-levels states are named qudits.

9.2 Principle of experiment

In this experiment, we will create and analyze high-dimensional entanglement. To create high-dimensional states in time-bin, we use a mode-locked laser and a non-linear crystal as in [59, 60]. However in the those experiments, the analysis of entanglement was done with Michelson [61], i.e. two dimensions interferometers. In this experiment, we will use high-dimensional interferometers. Such an interferometer is difficult to make, though we eventually realized high-dimensional Michelson interferometers (FIG. 9.2). We prefer to take the option to build Fabry-Perot like interferometer [61] (FIG. 9.3). In such an interferometer, the photons can make any number of multiple round-trips in the interferometers by using mirrors which partially reflect/transmit.

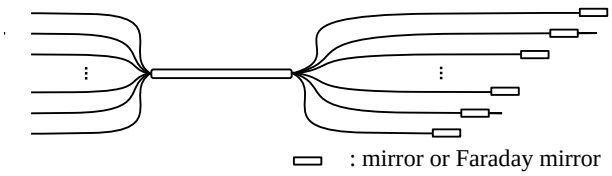


FIG. 9.2: *High dimensional Michelson interferometer.*

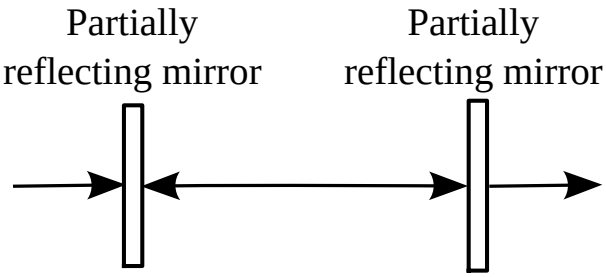


FIG. 9.3: *Fabry-Perot interferometer. Light can do multiple round trip between the two partially reflecting mirrors.*

In figure FIG. 9.4, we have a scheme showing the principle of the experiment. Pulses going out of the mode-locked laser pass through a non-linear crystal ($KNbO_3$ NLC). Each pulse can create photons pair by parametric down conversion of type I, with a certain probability. So, it's possible to create high-dimensional entanglement in time-bin by ensuring that only one pair is created in one of the d pulses defining the qudit. At the output of each photon is collected in its own mono-mode fiber. The photons arrive in their respective interferometer. The interferometer are built, so that the traveling time for one turn in the interferometer corresponds to $\Delta\tau = 1/f_{laser}$ where f_{laser} is the repetition frequency of the laser.

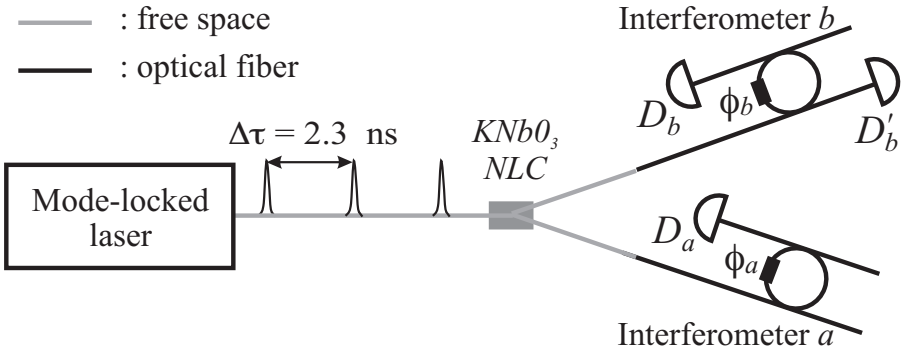


FIG. 9.4: *Scheme of principle.*

For the experiment, we measure the coincidences as a function of the time difference in arrival times for the detectors D_a-D_b and D_a-$D_b{}'$. For the detector D_a and D_b, the result is shown in figure FIG. 9.5.

In [62], we calculated the height of the different peaks. We obtain for the coincidences probability P_n between D_a-D_b:

$$\begin{aligned} P_{n=0} \equiv P_0 &\sim (t_{1a}t_{1b}t_{2a}t_{2b})^2 \left| \frac{1}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P_{n<0} &= (r_{2a}r_{1a})^{2|n|} P_0 \\ P_{n>0} &= (r_{2b}r_{1b})^{2n} P_0 \end{aligned} \tag{9.1}$$

where:

- by convention, $n = 0$ for the photons doing the same number of turns. On the left (right), the peaks are numbered -1, -2, ... (1, 2, ...)

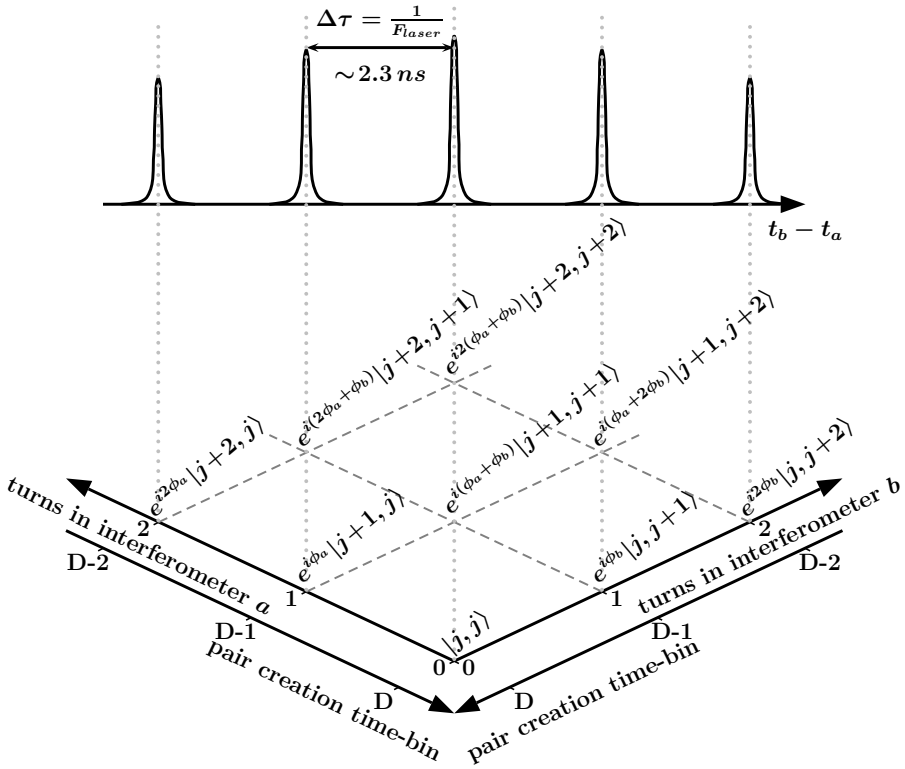


FIG. 9.5: *Coincidences as a function of the difference in arrival times for the two photons at detectors D_a and D_b. These correspond to the sum of different interfering terms, which are due to the different possibilities for each difference of time-of-arrival. The peaks on the left (right) of the central peak correspond to the cases when photons make more (less) turns in interferometer a than b.*

- t_{mx} and r_{mx} are the transmission and reflection amplitude of the first ($m = 1$) and second coupler of the interferometers. By convention, a reflected photon stays in the same fiber
- ϕ_a and ϕ_b are the phases per turn in interferometers a and b respectively

Two further remarks:

- to observe high-dimensional interferences, we have to chose $t_{mx} << r_{mx}$
- the phase dependance is the same for all of the peaks, thus, they oscillate synchronously.

For the coincidences D_a-$D_b{}'$, we obtain:

$$\begin{aligned} P'_{n=0} \equiv P'_0 &\sim \left(\frac{t_{1a}t_{2a}}{r_{1b}}\right)^2 \left| - r_{1b}^2 + \frac{t_{1b}t_{2b}r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P'_{n<0} &= (r_{2a}r_{1a})^{2(|n|-1)} P'_0 \\ P'_{n=1} \equiv P'_1 &\sim (t_{1a}t_{2a}t_{1b}^2 r_{2b})^2 \left| \frac{1}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}} \right|^2 \\ P'_{n>0} &= (r_{2b}r_{1b})^{2(n-1)} P'_1 \end{aligned} \tag{9.2}$$

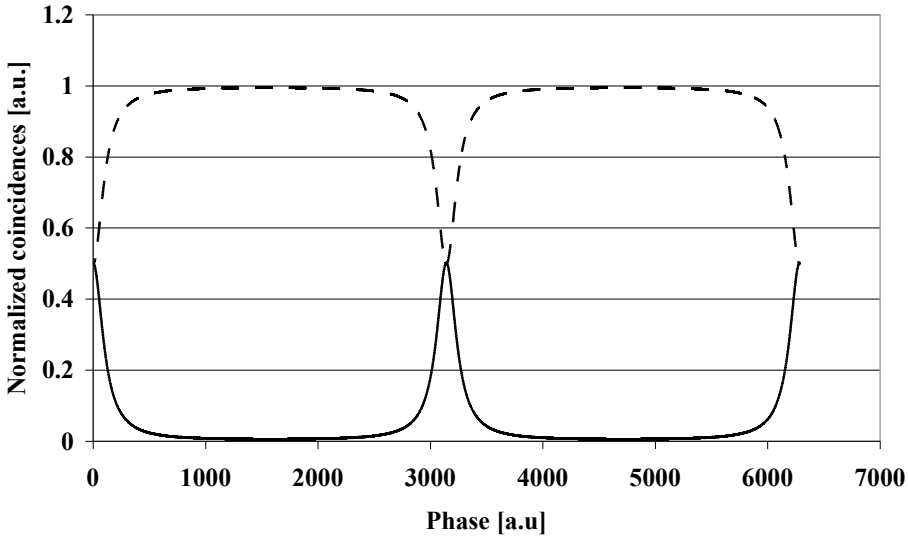


FIG. 9.6: *Simulation of normalized coincidences as a function of the phase. The solid line corresponds to coincidences D_a-D_b and the dashed one to the coincidences D_a-D'_b. We remark that the sum of the two curves is constant (conservation of energy) (no loss, $r_{mx} = \sqrt{0.9}$).*

where by convention, $n = 0$ for the photons doing the same number of complete turns. On the left (right), the peaks are numbered -1, -2, ... (1, 2, ...)

The P' terms also oscillate synchronously. However, P_n and P'_n oscillate in opposition to the phase. This behavior is logical, by supposing that there are no losses in the interferometer, the total number of photons outgoing of the interferometer must be constant by energy conservation. This is what we see in figure FIG. 9.6. We can also note that we have typical transmission curves for a Fabry-Perot interferometer, i.e. multi-path interferences.

9.3 Implementation

Figure 9.7 schematic depicts the experiment. An infinite train of pulses exits the mode-locked laser. With a mode-locked laser the phase between successive pulses is constant. We ensure that the laser is monochromatic at 532 nm with an equilateral prism EP and a pinhole P. In the non-linear crystal, non-degenerate photon pairs are produced at 810 nm/1550 nm with a probability lower than one percent per pulse of the pump laser. So we avoid multiple pair and the reduction of visibility associated. The dichroic mirror DM reflects the 810 nm photons and transmits those at 1550 nm. We optimize the coupling of the photons into the mono-mode fibers for each wavelength. There are two lenses in each of the coupling optic setup. The first one to collimate the beam and the second one to focalize the beam at the input of the fiber.

To avoid pump photon detection we must use filters. At 810 nm, there is a reflector at 532 nm, a RG 610 filter and a band-pass filter with a full with half-maximum (FWHM) of 10 nm and centered at 810 nm. At 1550 nm, there is a Si and a band-pass filters with FWHM of 10 nm and centered at 1550 nm. Here we have finished with the description of the source. Let's now see the description of the detection for the high-dimension states we have created.

The 1550 nm interferometer is made with two R/T=90/10 couplers (T: transmission proba-

bility, R: reflection probability). A polarization controller is put in the loop to optimize the interferences. To facilitate the length alignment of the second interferometer with the first one, the second interferometer is made with mono-mode fiber at 810 nm and with R/T=90/10 dielectrics mirrors deposed on the cleaved extremities. The fiber is cut a little shorter than required, within a few tens of mm. Due to the elasticity of the fiber, it is possible to then align this interferometer with the first one by using a translation stage, for the coarse alignment, and a piezoelectric actuator for the fine alignment are used to stretch the fiber.

The 810 nm are detected with silicon single photon avalanche photodiodes (APD). These detections start the time-to-digital converter (TDC) and the InGaAs/InP APDs detectors. Gates of 50 ns are applied on the InGaAs/InP detectors. The TDC registers the coincidences.

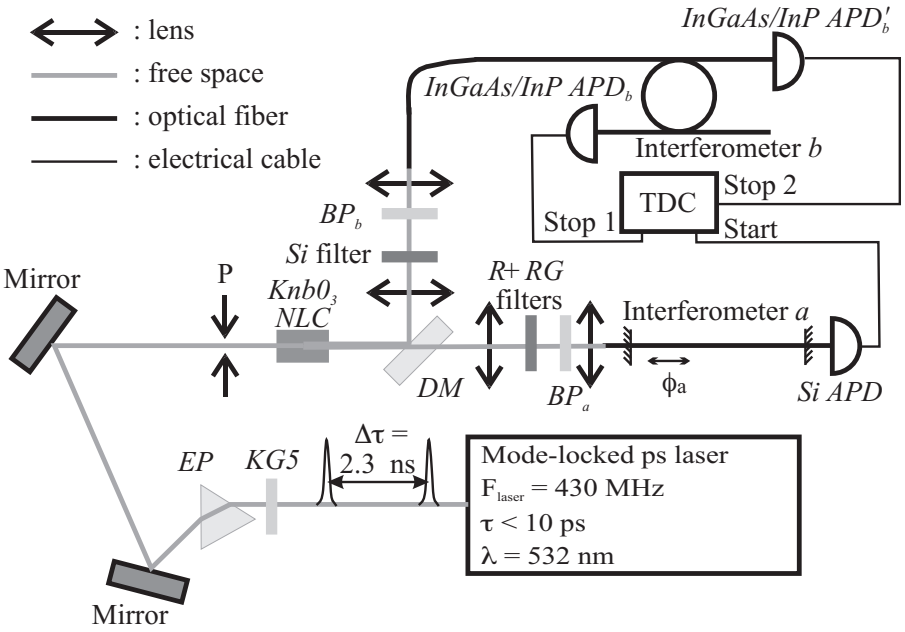


FIG. 9.7: *Implementation for high-dimensional entanglement. KG5 : filter; EP : equilateral prism; P : pinhole; $KNb0_3$ NLC : non-linear crystal of potassium niobate; BP_A et BP_B : band-pass filters. For details, see text.*

The alignment of the two interferometers is the first critical point. In practice, the alignment is done with low coherence interferometry using an additional bulk interferometer. The principle is presented in the figure FIG. 9.8. We use a source followed by the two interferometers in series and then a detection system. For the alignment between interferometer *b* and the additional interferometer, we use a LED for the source and polarization mode dispersion analyser, for the detection. In fact, we only use the fact that there is an interferometer in the PMD analyzer and we can scan the length of one arm. When the alignment is not perfect, there is three peaks on the PMD analyser. When the alignment is correct, there is only one peak on the PMD analyser.

For the alignment of interferometer *a* with the additional interferometer, the source is a LED and for the detector, we use a single-photon detector. We need to change of detector because PMD analyzer doesn't work at 810 nm. We change the length of the interferometer to align and when they are aligned within the coherence length of the LED, we measure large fluctuation of the detection rate.

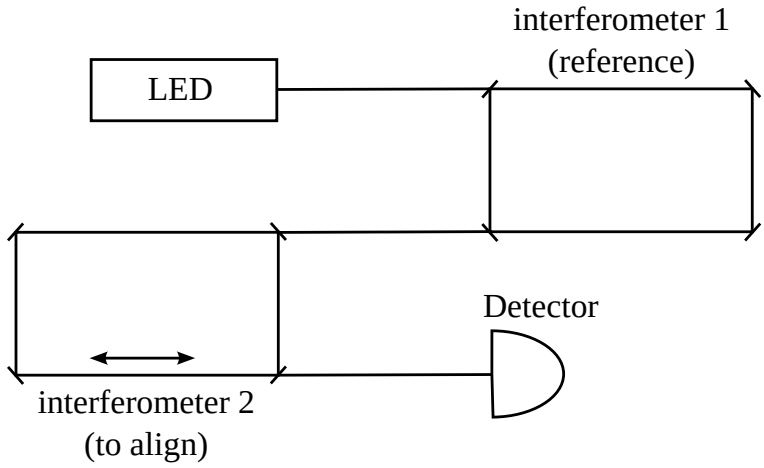


FIG. 9.8: *Low coherence interferometry.*

The cavity of the laser is also align with the additional bulk interferometer by directly sending the light in the bulk interferometer and looking at the fluctuation in detection power on classical detectors at the output.

The most delicate alignment is done for the a and b interferometers which has to be aligned within the coherence length of the photon pairs, about $120\,\mu$m. The alignment with the pump is less critical, because the coherence length of the pump is around 2 nm in fibers.

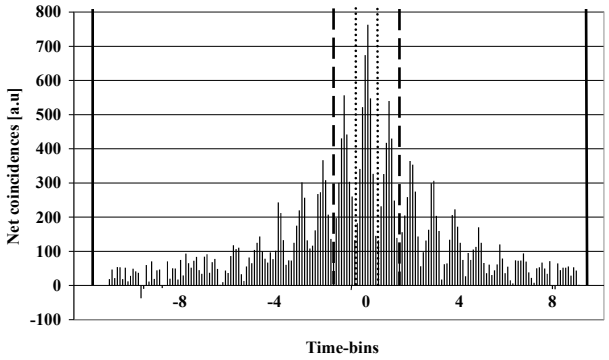
9.4 Experimental results

The accumulated coincidences D_a-D_b and D_a-$D_b{}'$ are presented in figure FIG. 9.9. The vertical lines in the figure FIG. 9.9(a) define the different time windows used for figure FIG. 9.10. The solid, dashed or dotted ones, respectively, define the the coincidences windows for the entire gate, three peaks or one peak respectively.

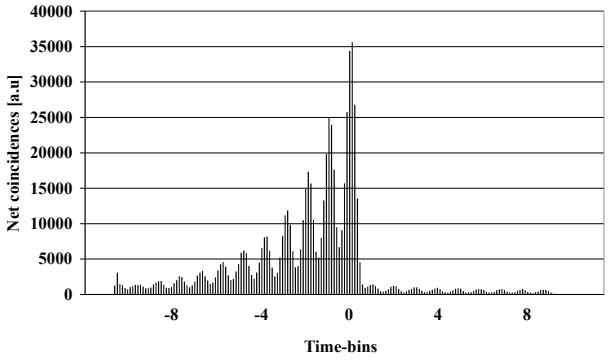
The next figure, FIG. 9.10, presents the coincidences between D_a and D_b as a function of the time, i.e. as a function of the phase. Effectively, we change the voltage on the piezoelectric actuator for each time which changes the fiber length and hence the phase in the interferometer a. As expected, we find typical curves of Fabry-Perot interferometer, the signature of high dimensional entanglement in this system. We also note that the central peak, the three central peaks and all peaks within the entire gate oscillate synchronously as expected from theory.

On the figure FIG. 9.11, we have the coincidences D_a-D_b and D_a-$D_b{}'$ for the entire gate, as well as numerical simulations. For the simulations, we take into account some experimental limitations :

- there are around 5 % of loss per round trip in the interferometers,
- the light is not monochromatic, hence the phase is not constant. We consider a FHWM of 10 nm at 1550 nm corresponding to a FWHM of 5.4 nm at 810 nm,
- small fluctuation of the temperature induce phase variation. We assume gaussian phase fluctuations with FWHM of $\pi/8$.



(a) Coincidences D_a-D_b.



(b) Coincidences D_a-D'_b.

FIG. 9.9: *Net coincidences as a function of the difference in arrival time. As $T << R$, in case (a) the accumulated coincidences are lower than in the case (b).*

The problem of polarization alignment haven't be taken into account. However, we attempted to align the polarization in the interferometer b using a polarization controller and we try to limit the birefringence in the interferometer a [62].

The theoretical and experimental results are quite close. The differences could be a consequence of the fact that simulations don't take into account all the effects (polarization, for example). Therefore, we can consider that we have created and measured high-dimensional entanglement.

9.5 Conclusion

In this experiment, we have demonstrated high-dimensional time-bin entanglement. The creation of high-dimensional entanglement is relatively easy, using the mode-locked laser and a non-linear crystal. However, the analysis is more difficult. The realization and alignment of interferometers is not easy.

Therefore, in conclusion, even given some of the theoretical advantages with high-dimensional systems, the use for an application in quantum information protocols seems improbable. The additional experimental difficulty induce by high-dimensional systems exceeds the advantages

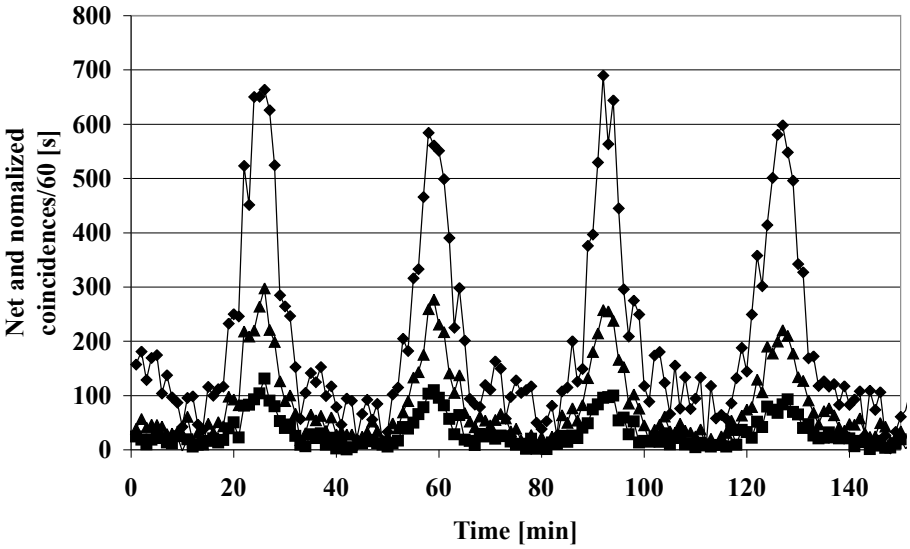


FIG. 9.10: *Normalized and net coincidences between D_a-D_b. Interferences for the central peak (♦), the three central peaks (▲) and the entire gate (♦).*

in comparison with two dimension systems.

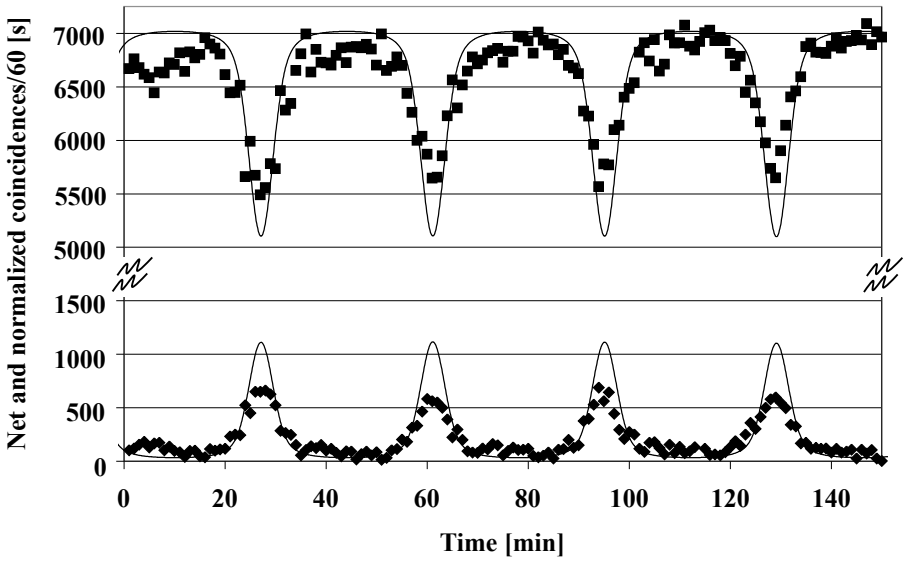


FIG. 9.11: *Comparison between experimental results and numerical simulations.* ♦ *: coincidences* D_a-D_b; ■ *: coincidences* D_a-D'_b. *See text for details*

Chapter 10

Conclusion

In this thesis, we studied effects flowing from quantum mechanics. The quantum properties like that of quantum coherence, quantum correlations, quantum superpositions or the perturbations induced during the measurement of quantum objects and how they can be used in the field of quantum information. Quantum information takes advantage of quantum properties to obtain more powerful results than with classical information.

Among the subjects flowing from this field, one is at the point of reaching the real world : quantum cryptography or quantum key distribution. With quantum key distribution and one-time pad protocol, it is possible to obtain perfectly and provably secure communications. Two start-up companies already sell commercial products [9, 10]. We can note that numerous companies from the classical information domain (Fujitsu, HP, IBM, Mitsubishi, NEC, Toshiba, ...) are interested in quantum information. So the field seems to have a promising future.

But let's go back to the main results obtained during this PhD thesis. In this thesis we studied different problems where quantum interferences plays a role. We particularly studied the possibility to uses them in quantum information protocols.

In chapter 7, we studied the plug&play system for quantum key distribution, an auto-stabilized and auto-aligned system. This experiment was really the most applied part of this thesis, but it exploited fundamental properties of quantum mechanics: quantum interferences and perturbations induced during the measurement of a quantum state. Quantum interferences of coherent weak pulses allow us to generate the key between two distant people. The security relies on the fact that, because of perturbations of quantum state (weak pulses in our case) during the measurement process, quantum interferences disappear. In this experiment, we developed a quantum key distribution prototype and we tested it on installed standard fiber in the Swisscom network. The system, working at 5 MHz, was tested under a lake, terrestrially and using aerial fibers. We confirmed that the auto-stabilization and auto-alignment work well in each of the different cases. We estimated a net key rate of 50 Hz over a distance of 67 km. This system has been further developed to obtain a fully functional commercially available system [9].

In chapter 8, we proposed a new protocol for quantum cryptography. This new protocol allows for a simpler implementation and higher key rates. The sender emits either empty (0) or weak coherent pulses (μ). Two non-orthogonal qubits, sequences 0μ and $\mu 0$, are then encoded in time. The better discrimination between the two states corresponds to a simple time-of arrival measurement which allows us to generate the key. To ensure the security

of the system, the quantum coherence of successive non-empty pulse is checked with an interferometer. This protocol is resistant to photon number splitting (PNS) attack. Indeed, for this protocol, a PNS attack is equivalent to a intercept-resend attack, an individual one. Hence, quantum coherence between successive μ pulses is broken. In a proof-of-principle experiment we demonstrated the operation of the system. After this first experiment, we developed a new system working at 760 MHz (380 MHz for logical bits). We succeed in modulation of the data, but we still have some problems with the detection. In a new realization, currently being developed, these problems should be resolved and the system should allow for a raw key exchange in the next months. In the next year, for the SECOQC project [41], the system should be fully functional with error correction, privacy amplification and authentication.

Finally, in chapter 9, we studied high-dimensional interferences from a more fundamental point of view. In this experiment, we created high-dimensional *time-bin* entanglement using a mode-locked laser and a non-linear crystal. The analysis was performed using two Fabry-Perot interferometers, so creating a Fabry-Perot like two-photon interferometer. By registering the coincidences at the outputs of the interferometers and by varying the phase in one interferometer, we demonstrate high-dimensional entanglement. This last experiment was made to study fundamental effects, which could also be used for new protocols of quantum information. However a practical application in the near future doesn't seem to be possible, because of the experimental complexity.

To conclude, over the last years, tremendous progress have already be done in this new field of quantum information and we can only hope that in the coming decades, new ideas will emerge in this field that allow for even more applications of fundamental physical properties in daily life.

Bibliographie / Bibliography

[1] M. Planck. Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum. *Verhandl. Deutsch. phys. Ges.*, 2 :237–245, 1900.

[2] A. Einstein. Über einen die Erzeugung und Verwandlung des Lichts betreffenden heuristischen Gesichtspunkt. *Ann. Phys.*, 17 :132–148, 1905.

[3] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43 :172–198, 1927.

[4] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete ? *Phys. Rev.*, 47 :777–780, 1935.

[5] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38 :447–452, 1964.

[6] S. J. Freedmann and J. F. Clauser. Experimental test of local hidden variable theories. *Phys. Rev. Lett.*, 28 :938–941, 1972.

[7] E. S. Fry and R. C. Thompson. Experimental test of local hidden variable theories. *Phys. Rev. Lett.*, 37 :465–468, 1976.

[8] A. Aspect, J. Dalibard, and G. Roger. Experimental test of bell ?s inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49 :1804–1807, 1982.

[9] www.idquantique.com.

[10] www.magiqtech.com.

[11] S. Singh. *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* Anchor, 2000.

[12] G.S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Electr. Eng.*, XLV :109–115, 1926.

[13] C. Bennett and G. Brassard. Quantum cryptography : Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, New York, 1984. IEEE.

[14] S. Wiesner. Conjugate coding. *Sigact News*, 15 :78–88, 1983. Ce papier, écrit dans les années 70, n'est paru que plus de 10 ans plus tard.

[15] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5 :3–28, 1992.

[16] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68 :3121, 1992.

[17] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67 :661–663, 1991.

[18] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1) :145–51, January 2002.

[19] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886) :802–803, October 1982.

[20] P. W. Milonni and M. L. Hardies. Photons cannot always be replicated. *Phys. Lett. A*, 92(7) :321–322, November 1982.

[21] V. Buzek and M. Hillery. Quantum copying : Beyond the no-cloning theorem. *Phys. Rev. A*, 54 :1844–1852, 1996.

[22] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin. Quantum cloning. *Rev. Mod. Phys.*, 77(4) :1225–32, October 2005.

[23] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85 :441–444, 2000.

[24] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret key rate for qkd protocols using one–way classical communication. *Phys. Rev. Lett.*, 95 :080501, 2005.

[25] A. Muller, T.Herzog, B. Huttner, W.Tittel, H. Zbinden, and N. Gisin. "plug and play" systems for quantum cryptography. *Appl. Phys. Lett.*, 70 :793–795, 1997.

[26] G. Ribordy, J-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Automated "plug & play" quantum key distribution. *Electr. Lett.*, 34 :2116–2117, 1998.

[27] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Fast and user-friendly quantum key distribution. *J. Mod. Opt.*, 47 :517–531, 2000.

[28] W.-Y. Hwa ng. Quantum key distribut ion with high loss : Toward global secure communication. *Phys. Rev. Lett.*, 91 :057901, 2003.

[29] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 2004.

[30] Hoi-Kwong LO, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94 :230504, 2005.

[31] www.ellisys.com.

[32] S. Cova and A. Lacaita. Trapping phenomena in avalanche photodiodes on nanosecond scale. *IEEE Electron Device Letters*, 12 :685–687, 1991.

[33] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity, and T. Wall. Quantum key distribution over 67 km with a plug&play system. *J. Mod. Opt.*, 48, 2001.

[34] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4 :41.1–41.8, 2002.

[35] S.Félix, N. Gisin, A. Stefanov, and H. Zbinden. Faint laser quantum key distribution : eavesdropping exploiting multiphoton pulses. *J. Mod. Opt.*, 48 :2009–2022, 2001.

[36] T. Debuisschert and W. Boucher. Time coding protocols for quantum key distribution. *Phys. Rev. A*, 70 :042306, 2004.

[37] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani. Towards practical and fast quantum cryptography. *http ://lanl.arxiv.org/pdf/quant-ph/0411022*, 2004.

[38] G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85 :1330, 2000.

[39] N. Lutkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61 :052304, 2000.

[40] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.*, 87 :194108, 2005.

[41] www.secoqc.net.

[42] www.princetonlightwave.com.

[43] http ://www.sensorsinc.com.

[44] Eleni Diamanti, Hiroki Takesue, Toshimori Honjo, Kyo Inoue, and Yoshihisa Yamamoto. Performance of various quantum key distribution systems using 1.55μm up-conversion single-photon detectors. *Physical Review A*, 72 :052311, 2005.

[45] R T Thew, S Tanzilli, L Krainer, S C Zeller, A Rochas, I Rech, S Cova, H Zbinden, and N Gisin. Low jitter up-conversion detectors for telecom wavelength ghz qkd. *New Journ. Phys.*, 8, 2006.

[46] G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and Roman Sobolewski. Picosecond superconducting single-photon optical detector. *App. Phys. Lett.*, 79 :705–707, 2001.

[47] A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smirnov, B. Voronov, G. N. Gol'tsman, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Sĺysz, A. Pearlman, A. Verevkin, and Roman Sobolewski. Sensitivity and gigahertz counting performance of nbn superconducting single-photon detectors. *App. Phys. Lett.*, 84 :5338–5340, 2004.

[48] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88(12) :127902, 2002.

[49] S. Massar. Non locality, closing the detection loophole and communication complexity. *Phys. Rev. A*, 65 :032121, 2002.

[50] D. Kaszlikowski, P. Gnacinski, M. Żukowski, W. Miklaszewski, and A. Zeilinger. Violations of local realism by two entangled n-dimensional systems are stronger than for two qubits. *Phys. Rev. Lett.*, 85 :4418–4421, 2000.

[51] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88(4) :040404, 2002.

[52] D. F. Walls and G. J. Milburn. *Quantum Optics*. Springer-Verlag, 1994.

[53] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, 1995.

[54] A. Lamas-Linares, J.C.Howell, and D.Bouwmeester. Stimulated emission of polarization-entangled photons. *Nature*, 412 :887–890, 2001.

[55] J. C. Howell, A. Lamas-Linares, and D. Bouwmeester. Experimental violation of a spin-1 bell inequality using maximally entangled four-photon states. *Phys. Rev. Lett.*, 88(3) :030401, 2002.

[56] H. Weinfurter and M. Żukowski. Four-photon entanglement from down-conversion. *Phys. Rev. A*, 64 :010102, 2001.

[57] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412 :313–316, 2001.

[58] A. Vaziri, G. Weihs, and A. Zeilinger. Superpositions of the orbital angular momentum for applications in quantum experiments. *J. Opt. B : Quantum Semiclass. Opt*, 4 :S47–S51, 2002.

[59] H. de Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin. Creating high dimensional time-bin entanglement using mode-locked lasers. *Quantum Inf. Comput.*, 2(6) :425–433, 2002.

[60] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin. Tailoring photonic entanglement in high-dimensional hilbert spaces. *Phys. Rev. A*, 69 :050304, 2004.

[61] M. Born and E. Wolf. *Principle of Optics - 7th edition*. Cambridge University Press, 1999.

[62] D. Stucki, H. Zbinden, and N. Gisin. A Fabry-Perot-like two-photon interferometer for high-dimensional time-bin entanglement. *J. Mod. Opt.*, 52(18) :2637–2648, 2005.

Troisième partie

Annexes / Appendix

Liste des publications / Publication list

1. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, **4,** 41.1, 2002.

2. Grégoire Ribordy, Nicolas Gisin, Olivier Guinnard, Damien Stucki, Mark Wegmuller and Hugo Zbinden. Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes : current performance. *J. Mod. Opt.*, **51,** 1381–1398, 2004

3. Nicolas Gisin, Grégoire Ribordy, Hugo Zbinden, Damien Stucki, Nicolas Brunner and Valerio Scarani. Towards practical and fast Quantum Cryptography. *quant-ph/0411022*, 2004.

4. D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.*, **87,** 2005.

5. D. Stucki H. Zbinden and N. Gisin. A Fabry-Perot-like two-photon interferometer for high-dimensional time-bin entanglement. *J. Mod. Opt.*, **52,** 2637–2648, 2005

Autres contributions / Others contributions

Conférences / Conferences

1. D. Stucki, H. Zbinden et N. Gisin. A Fabry-Perot like two-photon interferometer for high-dimensional time-bin entanglement. *Physics 2005*, Warwick, 2005.

2. D. Stucki, N. Gisin et H. Zbinden. Coherent one-way Quantum Cryptography. *Réunion de la société suisse de physique*, Lausanne, 2006.

Publications

New Journal of Physics
An Institute of Physics and Deutsche Physikalische Gesellschaft Journal

Quantum key distribution over 67 km with a plug&play system

D Stucki[1], N Gisin[1], O Guinnard[1,2], G Ribordy[1,2] and H Zbinden[1]

[1] GAP-Optique, University of Geneva, rue de l'Ecole-de-Médecine 20, CH-1211 Geneva 4, Switzerland
[2] id Quantique SA, rue Cingria 10, CH-1205 Geneva, Switzerland
E-mail: hugo.zbinden@physics.unige.ch

New Journal of Physics **4** (2002) 41.1–41.8 (http://www.njp.org/)
Received 7 March 2002
Published 12 July 2002

Abstract. We present a fibre-optical quantum key distribution system. It works at 1550 nm and is based on the plug&play set-up. We tested the stability under field conditions using aerial and terrestrial cables and performed a key exchange over 67 km between Geneva and Lausanne.

1. Introduction

Quantum cryptography or, more exactly, quantum key distribution (QKD) is the most advanced subject in the field of quantum information technologies. Since the introduction of the BB84 protocol by Bennett and Brassard in 1984 [1] and their first implementation in 1992 [2], many experiments have been performed by numerous groups (see e.g. [3] for a review). However, to our knowledge, all experiments to date have been performed in laboratories or used laboratory equipment (e.g. liquid nitrogen cooled detectors) or needed frequent alignments (e.g. control of polarization or phase). In this paper, we present a turn-key, fibre-optic QKD-prototype that fits into two 19 inch boxes, one for Alice and one for Bob (see figure 1). We tested the stability of the auto-compensating plug&play (p&p) system [4] over installed terrestrial and aerial cables. Keys were exchanged over a distance of 67 km.

We start with a short introduction to the p&p auto-compensating set-up and describe the features of the prototype. We then recall the relevant parameters of a QKD system and briefly discuss some security issues. Finally the results of the field tests are presented.

2. Plug&play prototype

Let us recall the principle of the so-called p&p auto-compensating set-up [4]–[8], where the key is encoded in the phase between two pulses travelling from Bob to Alice and back (see figure 2).

1367-2630/02/000041+8$30.00

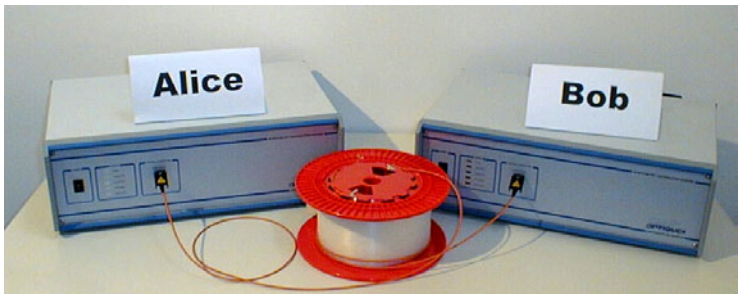


Figure 1. Picture of the p&p system.

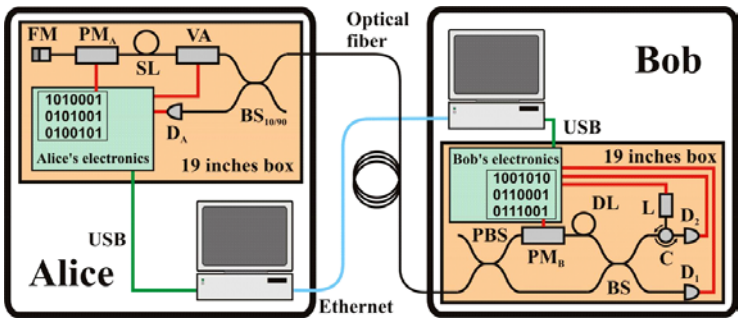


Figure 2. Schematic of the p&p prototype.

A strong laser pulse (@1550 nm) emitted at Bob is separated at a first $50/50$ beamsplitter (BS). The two pulses impinge on the input ports of a polarization beamsplitter (PBS), after having travelled through a short arm and a long arm, including a phase modulator (PM_B) and a 50 ns delay line (DL), respectively. All fibres and optical elements at Bob are polarization maintaining. The linear polarization is turned by 90° in the short arm, therefore the two pulses exit Bob's set-up by the same port of the PBS. The pulses travel down to Alice, are reflected on a Faraday mirror, attenuated and come back orthogonally polarized. In turn, both pulses now take the other path at Bob and arrive at the same time at the BS where they interfere. Then, they are detected either in D_1, or after passing through the circulator (C) in D_2. Since the two pulses take the same path, inside Bob in reversed order, this interferometer is auto-compensated. To implement the BB84 protocol, Alice applies a phase shift of 0 or π and $\frac{\pi}{2}$ or $\frac{3\pi}{2}$ on the second pulse with PM_A. Bob chooses the measurement basis by applying a 0 or $\frac{\pi}{2}$ shift on the first pulse on its way back.

The prototype is easy to use. The two boxes just have to be connected via an optical fibre. They are exclusively driven by two computers via the USB port. The two computers communicate via an ethernet/internet link. The system monitors on-line the temperature of the detectors, heat sinks and casings. The photon counters are Peltier-cooled, actively gated, InGaAs/InP APDs [9]. The dark count noise of the detectors is measured during the initialization (the dark count probability p_{dark} is $\approx 10^{-5}$ per gate). Although the set-up needs no optical alignment, the phases and the detection gates must be applied at the right time. Therefore, the system measures in a next step the length of the link (the operator has only to estimate the line's length to within 5 km). The variable attenuator (VA) at Alice is set to a low level and bright laser pulses are emitted by Bob. The time delay between the triggering of the laser

and a train of gates of the detectors is scanned until the reflected pulses are detected. The delays for the two 2.5 ns detection gates are adjusted, as well as the timing for the 50 ns pulse applied on the phasemodulator PM_B. In the p&p scheme, where pulses travel back and forth, (Rayleigh) backscattered light can considerably increase the noise. Therefore, the laser is not continuously pulsed, but trains of pulses are sent, the length of these trains corresponding to the length of the storage-line introduced for this purpose behind the attenuator at Alice's station [5]. Consequently, the backward propagating pulses no longer cross bright pulses in the fibre. For a storage line measuring approximately 10 km, a pulse train contains 480 pulses at a frequency of 5 MHz. A 90% coupler ($BS_{10/90}$) directs most of the incoming light pulses to a APD-detector module (D_A). It generates the trigger signal used to synchronize Alice's 20 MHz clock with the one of Bob. This synchronized clock allows Alice to apply a 50 ns pulse at the phasemodulator PM_A exactly when the second, weaker pulse passes. Only this second pulse contains phase information and must be attenuated below the one-photon-per-pulse level. Measuring the height of the incoming pulses with D_A would allow one to adjust the attenuator in order to obtain the correct average number of photons per outgoing pulse. For this purpose, the attenuator and the detector must be calibrated beforehand. In practice, we measure the incoming power with a power metre. Random numbers are generated on both sides with a quantum random number generator [10]. At Bob, clicks from each of the photon counters are written together with the index of the pulse into a buffer and transferred to the computer.

As a measure of security, the number of coincident clicks at both detectors is registered, which is important to limit beamsplitting attacks (see below). Moreover, the incoming power at Alice is continuously measured with D_A, in order to detect so-called Trojan horse attacks.

3. Key parameters in QKD

3.1. Key and error rates

The first important parameter is the raw key rate R_{raw} between Alice, the transmitter, and Bob, the receiver:

$$R_{raw} = q\nu\mu t_{AB} t_B \eta_B \tag{1}$$

where q depends on the implementation ($\frac{1}{2}$ for the BB84 protocol, because half the time Alice and Bob bases are not compatible), ν is the repetition frequency, μ is the average number of photons per pulse, t_{AB} is the transmission on the line Alice–Bob, t_B is Bob's internal transmission ($t_B \approx 0.6$) and η_B is Bob's detection efficiency ($\eta_B \approx 0.1$).

After R_{raw} the second most important parameter is the quantum bit error rate (*QBER*) which consists of four major contributions:

$$QBER = \frac{\text{false counts}}{\text{total counts}} = QBER_{opt} + QBER_{dark} + QBER_{after} + QBER_{stray}. \tag{2}$$

$QBER_{opt}$ is simply the probability for a photon to hit the wrong detector. It can be measured with strong pulses, by always applying the same phases and measuring the ratio of the count rates at the two detectors. This is a measure of the quality of the optical alignment of the polarization maintaining components and the stability of the fibre link. In the ideal case, $QBER_{opt}$ is independent of the fibre length. $QBER_{dark}$ and $QBER_{after}$, the errors due to dark counts and after-pulses, depend on the characteristics of the photon counters [9]. $QBER_{dark}$ is the most

important, it is the probability to have a dark count per gate p_{dark}, divided by the probability to have a click p_{det}:

$$QBER_{dark} \cong \frac{p_{dark}}{\mu t_{AB} t_B \eta_B}.$$

$QBER_{dark}$ increases with distance and consequently limits the range of QKD. $QBER_{after}$ is the probability to have an after-pulse $p_{after}(t)$ summed over all gates between two detections:

$$QBER_{after} \cong \sum_{n=0}^{n=\frac{1}{p_{det}}} p_{after}\left(\tau + n\frac{1}{\nu}\right) \tag{3}$$

where τ is the dead time, during which the detectors' gate are inhibited after each detection. The probability p_{after} depends on the type of APD as well as on the temperature, and decreases rapidly with time [9]. Nevertheless, for high pulse rates ($\nu = 5$ MHz) $QBER_{after}$ can become significant. For instance, for $p_{det} = 0.15\%$ (corresponding to about 7 dB loss with $\mu = 0.1$) we measured a $QBER_{after}$ of about 4%. By introducing a dead time τ of 4 μs (during this time, following a detection, no gates are applied), $QBER_{after}$ can be reduced to 1.5%. The bit rate R_{raw} in contrast, is only slightly reduced by a factor η_τ:

$$\eta_\tau = \frac{1}{1 + \nu p_{det} \tau} \lessapprox 1. \tag{4}$$

In this example, η_τ becomes 0.97 and 0.92, for 4 and 12 μs, respectively. In our prototype the dead time can be varied between 0 and 12 μs. The optimum dead time varies as a function of distance, in our measurements, however, we applied a constant dead time of 4 μs. Finally, $QBER_{stray}$, the errors induced by stray light, essentially Rayleigh back-scattered light, is a problem proper to the p&p set-up. It can be almost completely removed with the help of Alice's storage line and by sending trains of pulses as mentioned above. However, we have to introduce another factor η_{duty} that reduces our bit rate. It gives the duty cycle of the emitted pulse trains and depends on the length of Alice's DL l_D and the length of the fibre link l_{AB}:

$$\eta_{duty} = \frac{l_D}{l_{AB} + l_D}. \tag{5}$$

Hence with our prototype we can expect a raw rate of R_{raw} of about

$$R_{raw} = q\nu\mu t_{AB} t_B \eta_B \eta_{duty} \eta_\tau \approx 140 \text{ kHz}\left(\mu t_{AB} \frac{l_D}{l_{AB} + l_D}\right). \tag{6}$$

3.2. Error correction, privacy amplification and eavesdropping

The net secret key rate is further reduced during the error correction and privacy amplification processes by a factor of η_{dist}. We did not implement error correction and privacy amplification for our field tests, but we would like to roughly estimate the net key rate that could be obtained with our system. In theory, η_{dist} is simply given as the difference between the mutual information of Alice and Bob, I_{AB}, and Alice and Eve, I_{AE} [3]:

$$\eta_{dist} = I_{AB}(D) - I_{AE}. \tag{7}$$

Due to the errors, I_{AB} is smaller than 1. It is a function of the disturbance D, which is equal to the total $QBER$:

$$I_{AB} = 1 + D\log_2 D + (1 - D)\log_2(1 - D). \tag{8}$$

In the following we estimate the information of Eve, I_{AE}. In the line of Felix *et al* [11] we make the following assumptions:

• The measured *QBER* should, within the statistical limits, be equal to what is estimated according equation (2). If this is not the case, a real user will not proceed and blindly apply privacy amplification, he will stop the key exchange and look for the problem. If the *QBER* is within these limits, we attribute to Eve the $QBER_{opt}$ ($\lesssim 0.5\%$) plus the error (2σ) of the error estimation ($\lesssim 0.5\%$ for reasonably long keys), say 1% in total. In the case of perfect equipment of the eavesdropper and true single-photon source this error corresponds to an information of $\frac{2}{\ln 2} 1\% \cong 3\%$ [13].

• In the case of faint laser pulses and especially in the presence of high fibre losses, Eve can take advantage of multi-photon pulses and gain information while creating few or no errors [11]. In this case, it is important to measure the length of the line and to register coincident clicks at Bob's two detectors in order to limit Eve's possibilities. We assume that Eve possesses perfect technology, but cannot efficiently measure the number of photons without disturbing them and cannot store them. Furthermore, she uses fibres with losses as low as 0.15 dB km^{-1}. Under these assumptions one can calculate Eve's information per bit due to multi-photon pulses $I_{2\nu}$ and obtains about 0.06, 0.14 and 0.40 for, 5, 10 and 20 dB losses, respectively (for $\mu = 0.2$, 0.25 dB km^{-1} fibre loss and 10^8 pulses sent). Consequently, we obtain

$$I_{AE} \cong 0.03 + I_{2\nu}. \tag{9}$$

With equations (7)–(9) we can calculate a theoretical value of η_{dist}. In practice, η_{dist} will be smaller due to the limitations of the used algorithm. Privacy amplification can be performed without additional bit loss in contrast to error correction. For our estimation, we use the results of Tancewsky *et al* [12] for I'_{AB} after error correction

$$I'_{AB} = 1 + D\log_2 D - \tfrac{7}{2}D \tag{10}$$

which is in fact considerably smaller than I_{AB}. The information of Eve I_{AE} is reduced by the same factor $\frac{I'_{AB}}{I_{AB}}$, too. Finally, we obtain the following estimate of R_{net}:

$$\begin{aligned} R_{net} = \eta_{dist} R_{raw} &\cong (I_{AB} - I_{AE})\frac{I'_{AB}}{I_{AB}} R_{raw} \\ &\approx [1 + D\log_2 D - \tfrac{7}{2}D - (0.03 + I_{2\nu})(1 - (1-D)\log_2(1-D) - \tfrac{7}{2}D)]R_{raw}. \end{aligned} \tag{11}$$

4. Field measurements

4.1. Visibilities

In principle, the prototype can be tested in the laboratory by performing key exchange with different fibre losses and comparing the measured *QBER* and bit rates with the estimated values according to the simple formulae developed above. There are two motivations for field tests on installed cables. The first reason is to check if the auto-compensating set-up is robust in many different situations. Several effects could reduce the visibility of the interference. First, we have previously shown that Faraday rotation due to the Earth's magnetic field cannot considerably decrease the visibility [14]. Second, the time delay between the two pulses, travelling back and forth between Alice and Bob, could change due to a temperature drift. Let us assume that the temperature of the fibre increases with a rate $\theta[\frac{K}{h}]$. The time delay Δt between the two pulses

Table 1. Visibility measurements on different fibres.

Fibre	Length (km)	Loss (dB)	Visibility (%)
Geneva–Nyon (under lake)	22.0	4.8	99.70 ± 0.03
Geneva–Nyon (terrestrial)	22.6	7.4	99.81 ± 0.03
Nyon–Lausanne (terrestrial)	37.8	10.6	99.63 ± 0.05
Geneva–Lausanne (under lake) A	67.1	14.4	99.62 ± 0.06
Geneva–Lausanne (under lake) B	67.1	14.3	99.66 ± 0.05
Ste croix (aerial) A	8.7	3.8	99.70 ± 0.01
Ste croix (aerial) B	23.7	7.2	99.71 ± 0.01

is 54 ns. If θ is constant for the whole trip of the pulses, the second pulse will see a fibre that is longer by Δl:

$$\frac{\Delta l}{l} = \alpha \Delta T \tag{12}$$

$$\Delta l = \alpha 2 l_{AB} \Delta T = \alpha 2 l_{AB} \theta \Delta t. \tag{13}$$

With $\alpha = 10^{-5}[\frac{1}{K}]$, $l_{AB} = 50$ km, $\theta = 10[\frac{K}{h}]$ we obtain $150\ \mathrm{pm} \ll \lambda$. Hence this effect should be negligible especially since installed fibres have slow temperature drifts. In contrast, slow temperature induced length drifts can be large enough that frequent readjustment of Bob's delay becomes necessary. In fact, we noticed that during the heating up of Alice's box within the first hour of operation, the changes in the DL require a recalibration every 10 min or so. However, a bad synchronization of the detection window does not affect $QBER_{opt}$. Finally, mechanical stress could change the fibre length and/or birefringence. If the birefringence changes rapidly, the pulses are no longer orthogonally polarized at the input of Bob, despite the Faraday mirror. In this case the two pulses might suffer different losses at Bob's polarizing BS and the interference will no longer be perfect. Rapid changes in stress are unlikely in installed cables, a couple of meters below the surface. For this reason we also tested the prototype over an aerial cable. We had at our disposal two fibres of 4.35 km length, of which 2.5 km in an aerial cable. In order to amplify a hypothetical effect we put Alice and Bob side by side and passed twice through the cable (config. A). In configuration B we inserted one spool of about 15 km at the other end of the cable. Hence, the pulses made the following trip: Bob, the aerial cable, 15 km spool, the aerial cable, Alice (with her 10 km storage line), and back.

To measure the visibilities we sent relatively strong pulses (a couple of photons per pulse), always with the same compatible phase values and look at the counts on the two detectors, R_{right} and R_{wrong} (subtracting the counts due to detector noise). We then obtain the fringe visibility according to the standard definition

$$V = \frac{R_{right} - R_{wrong}}{R_{right} + R_{wrong}} \tag{14}$$

and the corresponding $QBER_{opt}$:

$$QBER_{opt} = \frac{1 - V}{2}. \tag{15}$$

Table 1 summarizes the result of visibility measurements over different cables. The indicated visibilities are the mean values over all four possible compatible phase settings. There was no

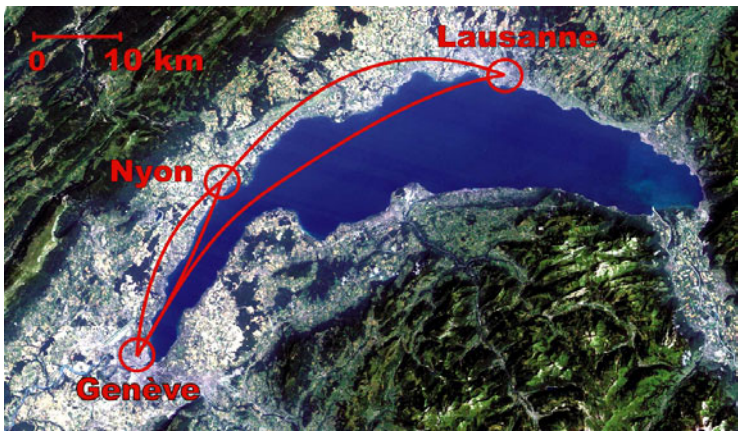


Figure 3. Satellite view of Lake Geneva with the cities of Geneva, Nyon and Lausanne.

Table 2. Overview of exchanged keys over different fibres ($\mu = 0.2$).

Fibre	Length (km)	Key (kbit)	R_{raw}(kHz)	*QBER* (%)	R_{net} (kHz)
Geneva–Nyon (under lake)	22.0	27.9	2.06	2.0 ± 0.1	1.51
Geneva–Nyon (terrestrial)	22.6	27.5	2.02	2.1 ± 0.1	1.39
Nyon–Lausanne (terrestrial)	37.8	25.1	0.50	3.9 ± 0.2	0.26
Geneva–Lausanne (under lake) A	67.1	12.9	0.15	6.1 ± 0.4	0.044
Geneva–Lausanne (under lake) B	67.1	12.9	0.16	5.6 ± 0.3	0.051
Ste Croix (aerial) A	8.7	63.8	6.29	3.0 ± 0.1	4.34
Ste Croix (aerial) B	23.7	117.6	2.32	3.0 ± 0.1	1.57

considerable decrease of the visibility in any fibre, hence the auto-compensating interferometers worked well under all conditions tested.

We tried to simulate an extremely unstable fibre link in the lab. For this purpose, we put a fibre-optical polarization scrambler (GAP-optique) at the output of Bob followed by 25 km of fibre. We measured the visibility as a function of the scrambler frequency. This frequency is defined as the number of complete circles that the vector of polarization would describe per second on the Poincaré sphere, if the birefringence changed uniformly. The visibility drops from 99.7 to 99.5% and 98% at frequencies of 40 and 100 Hz, respectively. This shows that the visibilities can decrease under rapid perturbations, however, it is unlikely to find such conditions using installed fibres.

4.2. Key exchange

We performed key exchange over different installed cables, the longest connecting the cities of Lausanne and Geneva (see figure 3). For testing we always used the same file of random numbers so that Bob could make the sifting and calculation of error rate without communication. We estimated the net key rate using equation (11). Table 2 gives an overview of the exchanged keys with $\mu = 0.2$.

We notice that secure key exchange is possible over more than 60 km with about 50 Hz of net key rate.

5. Conclusion

We presented a QKD prototype, which can be simply plugged into the wall, connected to a standard optical fibre and a computer via the USB port. It allows key exchange over more than 60 km, with a net key rate of about 50 bits s^{-1}. The system is commercially available [15].

Acknowledgments

We would like to thank Michel Peris and Christian Durussel from Swisscom for giving us access to their fibre links, as well as Laurent Guinnard and Mario Pasquali for their help with the software and firmware, Jean-Daniel Gautier and Claudio Barreiro for their help with the electronics. Finally, we thank Régis Caloz for the satellite picture. This work was supported by the Esprit project 28139 (EQCSPOT) through Swiss OFES and the NCCR 'Quantum Photonics'. We also acknowledge the support of Sun Microsystems.

References

[1] Bennett Ch H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)* pp 175–9

[2] Bennett Ch H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptograpy *Rev. Mod. Phys.* at press (Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Preprint* quant-ph/0101098)

[4] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 Plug&play systems for quantum cryptography *Appl. Phys. Lett.* **70** 793–5

[5] Ribordy G, Gautier J-D, Gisin N, Guinnard O and Zbinden H 2000 Fast and user-friendly quantum key distribution *J. Mod. Opt.* **47** 517–31

[6] Bethune D and Risk W 2000 An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light *IEEE J. Quantum Electron.* **36** 340–7

[7] Nielsen P M, Schori C, Sorensen J L, Savail L, Damgard I and Polzik E 2001 Experimental quantum key distribution with proven security against realistic attacks *J. Mod. Opt.* **48** 1921–42

[8] Bourennane M, Ljunggren D, Karlsson A, Jonsson P, Hening A and Ciscar J P 2000 Experimental long wavelength quantum cryptography: from single-photon transmission to key extraction protocols *J. Mod. Opt.* **47** 563–79

[9] Stucki D, Ribordy G, Stefanov A, Zbinden H, Rarity J G and Wall T 2001 Photon counting for quantum key distribution with Peltier cooled InGaAs APDs *J. Mod. Opt.* **48** 1967–82

[10] Stefanov A, Guinnard O, Guinnard L, Zbinden H and Gisin N 2000 Optical quantum random number generator *J. Mod. Opt.* **47** 595–8 (available from id Quantique, www.idquantique.com.)

[11] Félix S, Gisin N, Stefanov A and Zbinden H 2001 Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses *J. Mod. Opt.* **48** 2009–22

[12] Tancevski L, Slutsky B, Rao R and Fainman S 1997 *Proc. SPIE* **3228** 322

[13] Fuchs C A, Gisin N, Griffiths R B, Niu C S and Peres A 1997 Optimal eavesdropping in quantum cryptography: I. *Phys. Rev.* A **56** 1163–72

[14] Zbinden H, Gisin N, Huttner B, Muller A and Tittel W 2000 Practical aspects of quantum cryptographic key distribution *J. Cryptol.* **13** 207–20

[15] id Quantique SA, www.idquantique.com

JOURNAL OF MODERN OPTICS, 15 JUNE–10 JULY 2004
VOL. 51, NO. 9–10, 1381–1398

Taylor & Francis
Taylor & Francis Group

Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: current performance

GRÉGOIRE RIBORDY†, NICOLAS GISIN‡,
OLIVIER GUINNARD†, DAMIEN STUCKI‡,
MARK WEGMULLER‡ and HUGO ZBINDEN‡

†id Quantique SA, Rue Cingria 10, CH-1205 Geneve, Switzerland
‡Group of Applied Physics, University of Geneva,
Rue de l'Ecole-de-MÕdecine 20, CH-1211 Geneva 4, Switzerland

(*Received 28 July 2003*)

Abstract. InGaAs/InP avalanche photodiodes operated in the so-called Geiger mode currently represent the best solution to detect single-photon beyond 900 nm. They cover the 1100–1650 nm wavelength interval, which includes in particular the two windows used for optical communications (1310 and 1550 nm). A detection efficiency at 1550 nm of 10% with a dark count probability of 10^{-5} ns^{-1} is common, although significant variations can be encountered. At this efficiency, a FWHM temporal response of 300 ps can be achieved. Afterpulses caused by charges trapped by defects in the high field region of the junction constitute the main performance impairment phenomenon. They enhance the dark count probability and reduce out-of-gate detector blindness. These photon counting detectors can be used in optical time-domain reflectometry to improve the spatial resolution and reduce dead-zone effects. Quantum key distribution over metropolitan area networks also constitutes an important application.

1. Introduction

Avalanche photodiodes operated in a special so-called Geiger mode have the ability to detect single photons. Special devices called single-photon avalanche diodes (SPAD) have been developed, optimized for this regime and are commercially available. Silicon SPADs exhibit very good performance between 600 and 900 nm: quantum efficiencies for detecting single photons around 60%, dark counts in the absence of light below 100 counts per second and sub-nanosecond timing resolution. The excellent performance of silicon SPADs has enabled significant progress in luminescence studies, astronomy, sensor applications and fundamental research in physics.

However, if one wishes to pursue photon counting beyond 900 nm, for example at the longer telecom wavelengths of 1300 and 1550 nm, the situation is no longer so easy. Avalanche photodiodes optimized for single-photon detection in this part of the spectrum do not exist. Although near-infrared photomultiplier tubes having a spectral response extending to 1700 nm exist, their quantum efficiency does not exceed a fraction of a percent. For 1300 nm photons, germanium APDs have been extensively studied [1]. In order to have a reasonable dark count rate, these detectors must be cooled, usually with liquid nitrogen, to a temperature below

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online © 2004 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340410001677094

150 K, making them impractical for most applications. Furthermore, the cut-off wavelength of these APDs cooled to 77 K is around 1450 nm, making them unsuitable for use as photon counters for 1550 nm photons. More recently new approaches employing superconducting materials have been proposed and tested (see for example [2]). However, the cooling requirements of these detectors—4 K or lower—make them impractical for most applications.

The 0.73 eV bandgap of $In_{0.53}Ga_{0.47}As$ epitaxial layers grown and lattice matched to an InP substrate allows the fabrication of devices featuring single-photon sensitivity up to a wavelength of 1650 nm. Following the pioneering work of the group of Cova [3], quite a few groups have therefore turned their attention to using commercially available InGaAs/InP APDs, originally developed for optical communication applications, for photon counting at 1300 and 1550 nm (see for example [4, 5, 6]). This research has proved quite fruitful, and there are many applications emerging in optical metrology, in eye-safe range finding and in future quantum technologies. Moreover, commercial single-photon detection systems employing these InGaAs/InP APDs are now available [7].

In recent work, groups have relied almost exclusively on the EPM 239 InGaAs/InP APD manufactured by the Epitaxx division of JDS-Uniphase, which is currently the commercial photodiode exhibiting the best performance as a single-photon counter in the telecom wavelength region. This article describes the most recent results obtained with these APDs. Section 2 explains the general principles of single-photon detection with InGaAs/InP APDs. Section 3 discusses operation modes and quenching techniques. Section 4 presents typical performance of EPM 239 devices in Geiger mode. Applications both in the field of telecom instrumentation and quantum optics are then discussed in section 5.

2. Transforming single photons into macroscopic current pulses

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 p–i–n junction diode, which operates at zero or low reverse bias and provides no internal current gain. Although p–i–n 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 p–i–n 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 and creates 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. If the field is high enough, impact ionization can yield a self-sustaining current pulse. This multiplication phenomenon is known as an avalanche.

In the case of InGaAs/InP APDs the photons are absorbed in a narrow bandgap InGaAs layer (see figure 1). The photogenerated hole is then injected into the wider bandgap InP multiplication layer. Separate absorption and multiplication layers are designed to optimize the avalanche behaviour and minimize the associated excess noise factor. This also ensures that tunnelling breakdown in the narrow bandgap InGaAs layer occurring at field values lower than the threshold

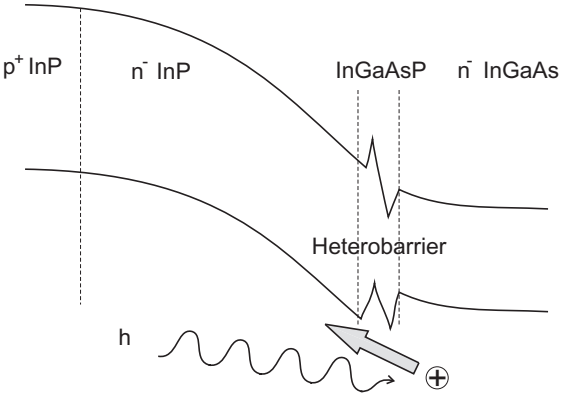


Figure 1. Schematic band diagram of a separate absorption and multiplication InGaAs/InP avalanche photodiode.

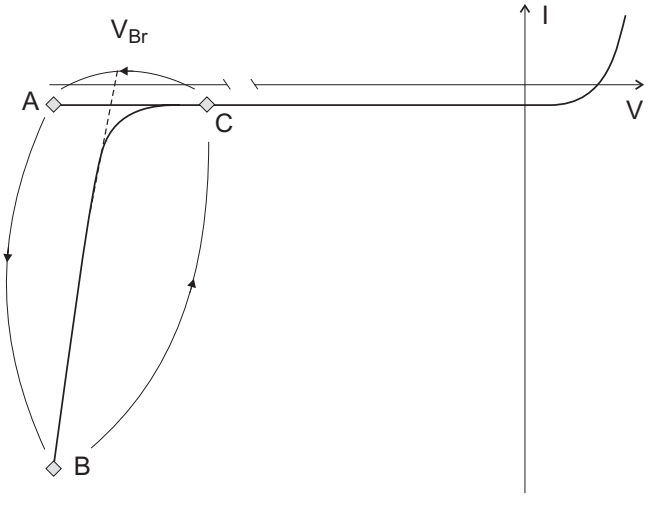


Figure 2. Diagram of the current–voltage (*I–V*) characteristics of an avalanche photodiode. When operated in Geiger mode, the APD is biased beyond breakdown voltage (point A) and remains in this metastable state until a primary electron–hole pair is created and triggers an avalanche (point B). This avalanche is quenched by lowering the bias voltage (point C). After a certain time, the excess bias voltage can be restored.

for avalanche multiplication does not impair function. Because of the bandgap difference between InGaAs and InP, a grading quaternary InGaAsP layer is used to smooth the band discontinuity, which could otherwise trap charge carriers and slow down temporal response.

For conventional optical communication applications, the reverse voltage applied is below the so-called breakdown voltage, the point where a self-sustaining avalanche current can be initiated by thermal fluctuations or tunnelling effects. The output signal is a linearly amplified copy of the input signal.

Figure 2 represents the *I–V* characteristics of an APD and illustrates how single-photon sensitivity can be achieved. The APD is biased, with an excess bias voltage, above the breakdown value and is in a metastable state (point A). In this

case, the amplification effectively becomes infinite, and even the absorption of a single photon has a non-zero probability of causing 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 time, the excess bias voltage is restored (point C to A) and the APD is again ready to detect a photon. This mode is also known as the Geiger mode.

The actual value of the breakdown voltage depends on the semiconductor material, the device structure and the temperature. For the EPM 239 APD, it ranges between 50 and 60 V. The excess bias voltage is typically a few volts and it influences most of the characteristics of the detector (detection efficiency, dark count probability, etc.).

3. Operation modes

When an avalanche is triggered, a current starts to flow through the device and rapidly reaches the milliampere regime. One must use proper electronic circuitry to sense the current pulse and quench the avalanche in order to avoid destruction of the device. After a time interval long enough for the photodiode to recover, the excess bias voltage must be restored to reactivate the detector. There are several ways to produce the quenching effect [8].

3.1. *Passive quenching*

The simplest quenching technique is called passive quenching. The APD is connected in series with a large load resistor (typically several tens or hundreds of kΩ) to pull the voltage across the photodiode below the breakdown value quickly after an avalanche current starts flowing across the junction. After the quenching, the APD capacitance is slowly recharged via the load resistor and the excess bias voltage is progressively restored.

Passive quenching does not allow very high bias voltage operation, which limits the achievable quantum detection efficiency (see below). Although quite efficient with Si and Ge APDs, this technique has not yielded good results with InGaAs/InP APDs [5]. The explanation probably lies in the strong afterpulsing effect (see below) encountered with this type of photodiode. This may of course change in the future as new APDs are developed.

3.2. *Active quenching*

When connected to an APD, an active quenching circuit senses the onset of an avalanche pulse and promptly reacts by lowering the bias voltage below the breakdown value. After a controlled hold-off time, the bias voltage is switched back to the normal excess bias value.

The basic advantage of this technique is that a high excess bias voltage value can be applied to the detector, making it possible to achieve high quantum detection efficiencies. The precisely defined duration of the avalanche pulse and of the dead time preceding the restoration of the bias voltage also constitute advantages. The disadvantage is linked to the fact that the circuitry is more complex and that the distance between the APD and the circuit must be as short

as possible to guarantee prompt quenching. This can prove difficult when the detector is cooled.

3.3. *Gated mode*

In many applications, the precise arrival time of a photon on the detector is known, making it possible to use a gated mode of operation. In this approach, the excess bias voltage across the APD is briefly raised above the breakdown voltage when a photon is expected. The duration of this gate is typically a few nanoseconds. Two such gates are separated by a longer hold-off time (typically more than 500 ns), during which the bias voltage is kept well below the breakdown voltage. Because of the possibility of applying a high excess bias voltage, this technique makes it possible to achieve high detection efficiencies and good timing resolutions. In addition, the fact that the detector is activated only for a short time period, allows one to limit dark count occurrences and to keep the afterpulse probability low.

Gated operation with longer gates (up to 100 ns) is also possible. This technique allows improvement of the duty cycle of the activation time of the detector. Furthermore feeding the detection signal into a time-to-amplitude converter allows monitoring of the temporal distribution of the recorded photons. However, because of the length of the gate, one cannot rely any longer on its end to quench the avalanche rapidly. One should thus resort to using long gates in conjunction with another quenching technique (passive or active) to ensure prompt quenching of the avalanches, in order to keep the afterpulse probability low.

Gated mode operation with short gate duration is recommended for every application where the arrival of the photons is precisely determined. By scanning the gate position, it can also be used in a scanning mode to investigate the distribution of the arrival time of photons.

When applying a gate pulse with steep rising and falling edges on an APD, a transient signal—resulting from the derivation of the gate pulse by the capacitance of the detector—is recorded (see figure 3). Avalanches—if present—will appear between the positive and the negative derivation pulses. The avalanches are then transformed into a logical signal by the use of a discriminator. When the rising edge is steep (typically < 500 ps), the height of the avalanche signal and derivation signal may be of the same order of magnitude, making it impossible to record one without the other. One possibility to reject the transient signal is to feed the discriminated signal into an AND gate [4] (figure 3). On the second input of this gate, one applies a pulse delayed with respect to the gate pulse and arriving after the positive transient. The results presented in this paper all use this technique.

Some groups have proposed other transient signal rejection techniques. Bethune and Risk use an arrangement allowing them to apply first a positive gate signal and second a negative gate signal, producing inversed transient signals. They then delay one and add the two resulting signals to obtain cancellation of the transient [9]. More recently, Tomita and Nakamura have tried subtracting the transient signals coming from two different APDs with a hybrid junction [10].

4. Geiger mode performance

A typical set-up for single-photon detection is shown in figure 4. It will be assumed below that the detector is operated in gated mode. A delay generator is

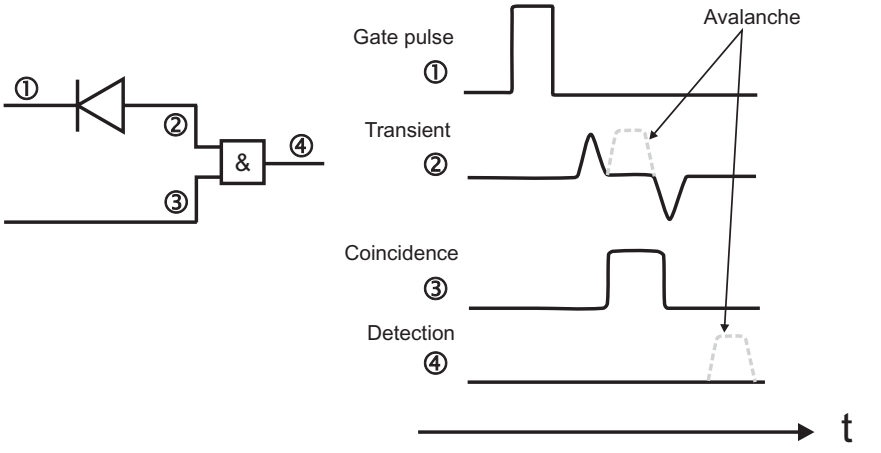


Figure 3. Transient signal suppression by the use of a coincidence circuit. Upon the application of a steep gate signal (1) on the APD, a transient signal (2)—possibly with an avalanche superimposed—is recorded and fed into an AND gate with a coincidence signal (3). If the delay is correctly set, the AND gate suppresses the positive transient while preserving the avalanche (4).

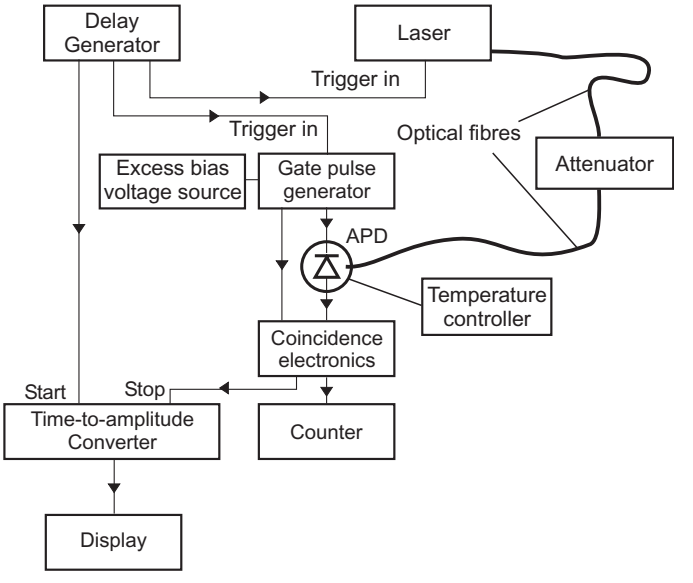


Figure 4. Set-up used for characterizing the performance of an APD in Geiger mode.

used to provide trigger signals for a pulsed light source and the gate pulse generator. The gate is sent onto the APD and the resulting signal picked up by the coincidence electronics. The device under test is placed between the light source and the detector, which are usually linked using optical fibres. The coincidence electronics is connected to a counter. The delay generator also provides a start signal for a time-to-amplitude converter, while the stop comes from the coincidence electronics.

4.1. *Quantum detection efficiency*

This set-up can be used for the characterization of the performance of APDs. In this case, the device under test is however replaced by an attenuator. The attenuation is selected so that on average one photon per pulse impinges on the detector.

The characterization procedure then consists in cooling the detector to a certain temperature and to record the detection efficiency as well as the dark count probability as a function of the excess bias voltage. For a given excess bias voltage value, one records the total avalanche probability p_{tot} when illuminating the detector with light pulses. These avalanches arise both from signal counts and dark counts. One then blocks the light and records the dark count probability p_{dc}. The detection efficiency η is expressed as

$$\eta = [\ln(p_{dc} - 1) - \ln(p_{tot} - 1)]/n, \tag{1}$$

where n is the average photon number per pulse. Equation (1) takes into account the fact that the probability distribution of the number of photons per pulse is Poissonian.

The Geiger mode quantum detection efficiency results from three different factors:

(a) the optical coupling efficiency from the optical fibre onto the active area of the detector;
(b) the probability that a photon is absorbed in the InGaAs absorption layer;
(c) the probability that the photogenerated carrier triggers an avalanche when crossing the multiplication zone.

Increasing the excess bias voltage has the effect of enhancing the avalanche triggering probability, which in turn results in increased detection efficiency.

The spectral dependency of the detection efficiency can be measured using a calibrated broadband light source followed by a monochromator. The excess bias voltage is set so that the detection efficiency is 10% at 1550 nm and the wavelength scanned. Figure 5 shows the result of this measurement. Single-photon detection is possible (efficiency > 2%) between 1100 and 1650 nm. The long wavelength cut-off comes from the fact the energy of the photons is not sufficient any longer to

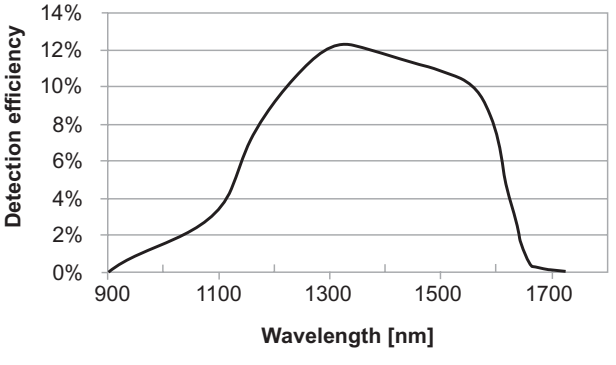


Figure 5. Quantum detection efficiency of the EPM 239 APD in Geiger mode as a function of the wavelength. The excess bias voltage was selected to set the detection efficiency at 10% for 1550 nm.

generate an electron–hole pair across the gap of the absorption layer. Photons are not absorbed in the InGaAs layer, which becomes transparent. At the other end of the spectrum, the short wavelength cut-off comes from the fact that when their energy becomes sufficient the photons are absorbed in the InP layer rather than in the InGaAs one (the APD is backlit through the InP substrate) and the photogenerated holes are not injected in the multiplication zone any longer.

4.2. *Dark counts*

In an APD, avalanches are not only caused by the absorption of a photon, but can also be randomly triggered by carriers generated in thermal, tunnelling or trapping processes taking place in the junction. They cause self-triggering effects called dark counts.

The easiest way to reduce dark counts is to cool the detector. This reduces the occurrence of thermally generated carriers. At low temperature, dark counts are thus dominated by carriers generated by band to band tunnelling and more importantly trapped charges (see below).

When selecting the operation temperature, one should take into account the following three factors. First, cooling the detector to a temperature that is too low can degrade its performance, because of the increase in the trapped charges' lifetime enhancing afterpulse probability. Second, low temperature can also impede its functioning. The breakdown voltage indeed decreases when the temperature is lowered. In order for the APD to work properly, the breakdown voltage must however remain larger than the reach-through voltage—the voltage for which the high-field region extends into the InGaAs absorption layer, which does not depend on the temperature. Finally, there should be a practical means of cooling the APD at the selected temperature. For most applications, thermo-electric cooling, making it possible to reach minimal temperatures around 200 or 210 K, is considered more practical and economical than liquid nitrogen cooling or other techniques.

In the gated mode, one typically quantifies the dark count's effect as a probability per gate. Alternatively it can also be expressed as a dark count probability per nanosecond of gate duration. This is useful when working with long gates.

Figure 6 shows this dark count probability per gate (2.5 ns) as a function of the detection efficiency (1550 nm) for several temperatures. The implicit parameter is the excess bias voltage. Both the dark count probability and the detection efficiency increase with the excess bias voltage. The graph clearly shows that dark count occurrence is reduced by cooling of the detector. The trigger frequency is 10 kHz and it was verified that it is sufficiently slow to ensure a negligible dark count enhancement by afterpulses. At a temperature of 223 K, this particular EPM 239 APD exhibits a dark count probability around 10^{-5} for a detection efficiency of 10%. Several EPM 239 APDs have been tested and it was found that the dark count probability exhibits significant differences between samples. This difference spans about one order of magnitude, with a dark count probability of the order of 10^{-4} for samples exhibiting poor performance.

4.3. *Afterpulses*

Perhaps the major problem limiting the performance of present InGaAs/InP APDs is the enhancement of the dark count probability by so-called afterpulses.

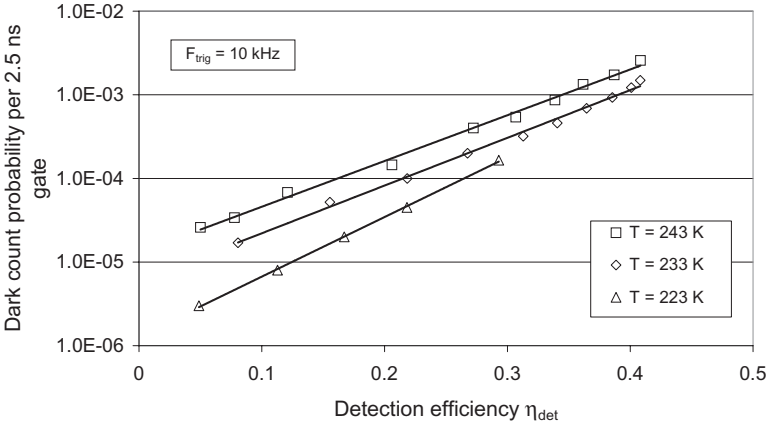


Figure 6. Dark count probability for the EPM 239 APD in gated mode (2.5 ns gate width) as a function of the quantum detection efficiency for three different temperatures. The implicit parameter is the excess bias voltage.

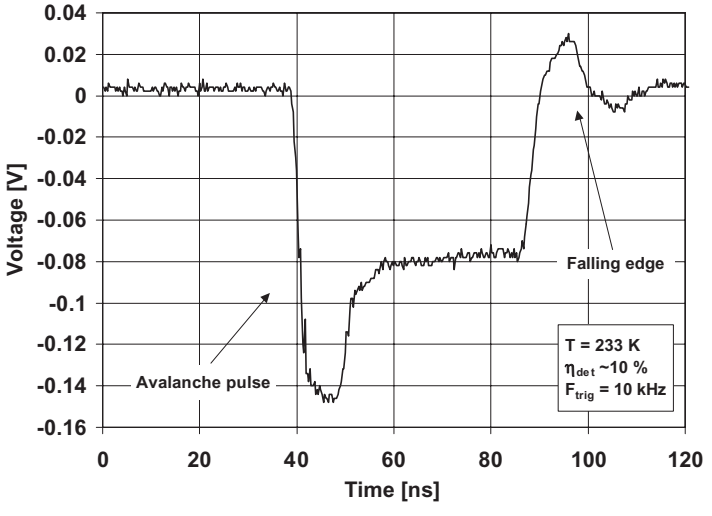


Figure 7. Avalanche pulse of the EPM 239 APD recorded with a digital oscilloscope. The gate width was 100 ns and the excess bias voltage was set to have a 10% efficiency at 1550nm.

This spurious effect arises from the trapping of charge carriers during an avalanche by trap levels inside the high field region of the junction where impact ionization occurs. When subsequently released, these trapped carriers can trigger a so-called afterpulse. The lifetime of the trapped charges is typically a few μs. The probability of these events is also proportional to the number of filled traps, which is in turn proportional to the charge crossing the junction in an avalanche before the quenching takes place. The total charge should thus be limited by ensuring prompt quenching of the avalanches.

In order to gain some insight on the trap filling process, one can follow the approach first introduced by Lacaita *et al*. [3] and look at the shape of the avalanche pulse (figure 7). The detector is operated in gated mode with a 100 ns

gate. A trace corresponding to a single avalanche pulse is then recorded with a digital oscilloscope. It shows the avalanche pulse and the falling edge transient (note that the rising edge transient is outside of the trace). The avalanche signal increases rapidly and reaches a maximum after 7.5 ns. At this point the signal decreases, indicating a change in the excess bias voltage applied to the junction. This decrease takes place in two steps. First a steep one lasting about 3 ns and resulting from the filling of the traps by the charges crossing the junction, which changes the charge distribution and increases the breakdown voltage. Second a slow decrease lasting until the quenching of the avalanche and indicating the heating of the junction by the flowing current, which also increases the breakdown voltage. This analysis shows that the quenching time should be smaller than about 5 ns in order to prevent significant filling of the traps. This illustrates why gated mode operation with gate duration of 2.5 ns is beneficial.

One can also investigate the impact of the gate amplitude on the afterpulse probability. This quantity is measured by sending a pair of gates on the APD separated by an adjustable time delay. The afterpulse probability is equal to the probability of registering an avalanche in the second gate when one was registered in the first one. Figure 8 shows this probability measured with gate amplitudes of 3, 4, 6 and 8 V in the case of long gates (20 ns). The short gate generator does indeed not allow for varying the amplitude, which is set at 7.5 V. In each case, the excess bias voltage is identical, yielding identical detection efficiency. The fact that the amplitudes of the gate differ means that the voltage during the off phases is different. It is clearly beneficial to work with a high amplitude gate, which indicates that a lower voltage across the junction reduces the lifetime of the trapped charges. The physical mechanisms behind this effect are still unclear. Although it was not possible to perform a similar measurement with shorter gates, it is expected that the conclusion will also hold in this case.

As mentioned previously, a decrease of the operation temperature of the APD translates into an increase of the lifetime of the trapped charges. This effect was

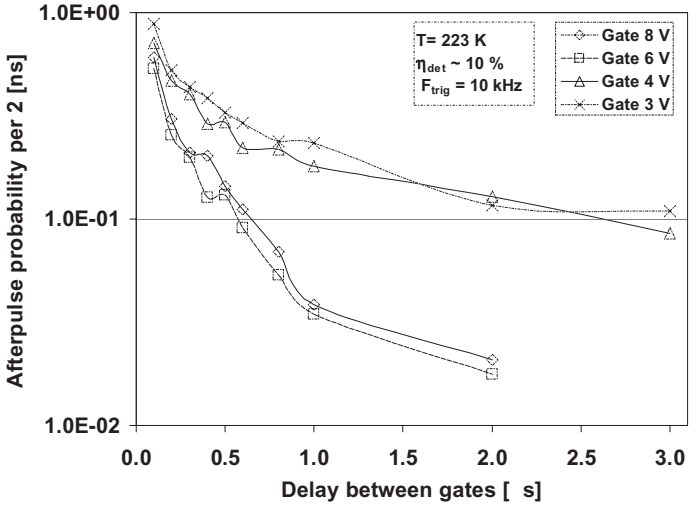


Figure 8. Afterpulse probability per 2 ns versus time delay between the two gates of a pair for 20 ns long gates of 3, 4, 6 and 8 V amplitude.

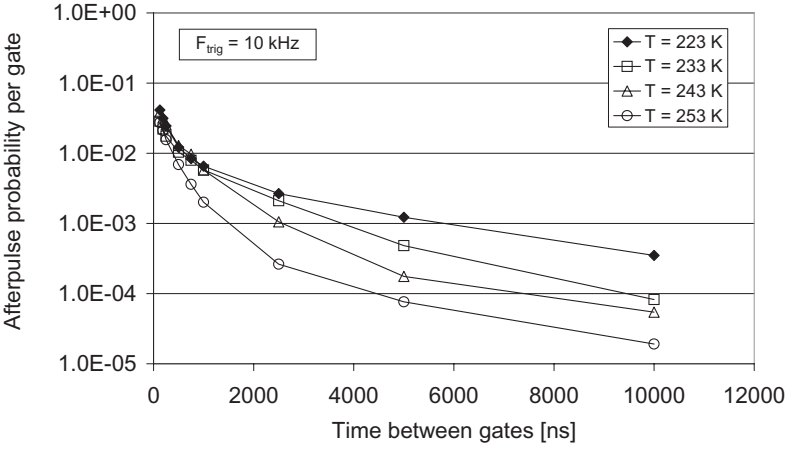


Figure 9. Afterpulse probability per 2.5 ns gate pulse versus time delay between the two gates of a pair for four different temperatures.

studied by sending pairs of short gates (2.5 ns) on the APD and by looking at coincidence counts as a function of the time interval. Figure 9 shows the results of the measurement. The afterpulse probability is shown for three temperatures. It confirms that the lifetime decreases when the temperature is increased. At 223 K and after 10 µs, the afterpulse probability is still of the order of 0.5×10^{-4}. Significant differences can be observed between different APD samples. The cooling temperature must thus be carefully chosen to minimize the total dark count probability, which depends on the trigger frequency. For most applications and current InGaAs/InP APDs, a temperature around 220 K yields good performance.

So far, the cure to get rid of the dark count enhancement by afterpulses has been to use the gated mode detection scheme (see above). If the voltage across the APD is kept below the breakdown voltage for a sufficiently long time interval, longer than the trap lifetime, between two subsequent gates, trap levels are empty and cannot trigger an avalanche. With typical trapping time in the µs range, however, the upper repetition frequency of InGaAs/InP APDs is limited to a few MHz. In most applications involving single-photon detection, the probability to detect a photon within a given gate is usually quite low. A good way to reduce the occurrence of afterpulses when working at a high trigger frequency is thus to use a dead time and inhibit gates for a certain time after each avalanche. To illustrate this effect, the probability of detecting an avalanche with a pulse containing on average one photon per pulse is measured for different gate durations and two trigger frequencies (10 and 100 kHz). The results are shown in figure 10. As the detection efficiency is 10%, one expects to obtain a probability of around 10%. This is the case when the trigger frequency is 10 kHz. Moreover, this probability should not depend on the trigger frequency. When this frequency is increased to 100 kHz, one sees that the probability increases. This is typical of count enhancement by afterpulses. The effect is particularly important for the longer gate durations (15.2% instead of 10.7% for a 100 ns gate), because in this case the avalanche is not quenched fast enough to prevent filling of the traps. The use of a 10 µs dead time strongly reduces this effect (11.4% for a 100 ns gate).

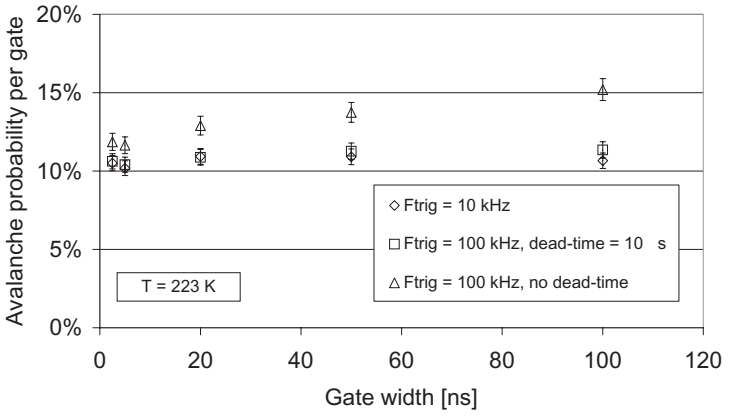


Figure 10. Avalanche probability with a pulse containing one photon on average for different gate widths. The different series correspond respectively to a repetition frequency of 10 kHz (◇), 100 kHz without dead time (△) and 100 kHz with a 10 μs dead time (□).

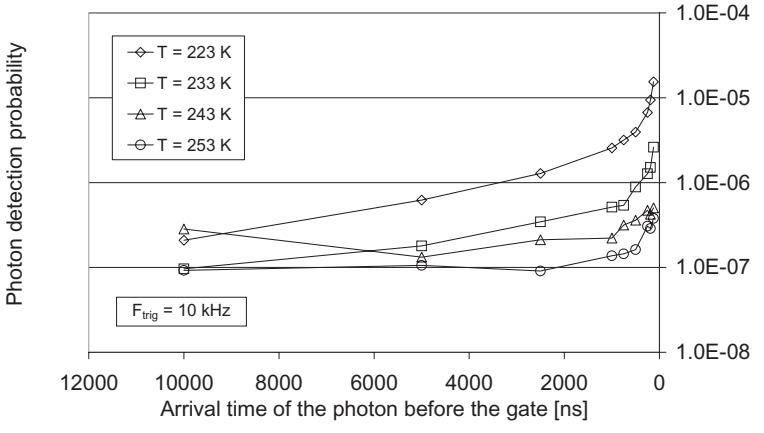


Figure 11. Detection probability of a photon impinging on the detector before the gate (2.5 ns) as a function of the delay between its arrival and the beginning of the gate. The different traces correspond to different temperatures.

Finally, a last effect of afterpulses is that the APD is not completely blind to photons impinging outside of the gate. In order to illustrate this, one can register the probability to detect a photon as a function of its time of arrival before the gate. Figure 11 shows the results of this measurement for several temperatures. If the arrival time is 0, the photon coincides with the gate and the detection probability is 10% (not plotted on the figure). If it arrives earlier, the probability drops steeply but is not zero. At a temperature 223 K, the probability is still of the order of 10^{-6} for an arrival time preceding the gate by 2 μs. Just like the afterpulse probability, this effect is enhanced by a reduction of the temperature. The fact that, upon arrival of the photon, the bias voltage is not zero, even though the APD is biased below the breakdown value and thus not in Geiger mode, can explain this phenomenon. The photon is absorbed and the photogenerated hole injected in the multiplication region. This results in the production of a current pulse, which

is however not self-sustaining. Just like in the case of an avalanche, the carriers crossing the junction can fill traps and their release subsequently trigger an avalanche. Although this out-of-gate detection probability is quite small, one has to be careful when the detector is illuminated with intense light pulses outside of the gate or with a moderate continuous-wave light flux.

4.4. *Temporal response*

For many applications, the timing resolution of the detector is also important. It depends on the time it takes for a photogenerated carrier to be swept out of the absorption zone into the multiplication zone and to trigger an avalanche. Because of the statistical nature of the avalanche phenomenon, this time will vary from one avalanche to the other.

In order to quantify its temporal response, the detector is operated in gated mode with long gates (100 ns). Short and weak light pulses are sent to the detector. The spread of the onset of the avalanche pulses is monitored with a time-to-amplitude converter. The width of the recorded response is equal to the square root of the sum of the squares of the individual components, mainly the laser pulse width (120 ps) and the detector temporal response. The intrinsic response time of the detector can thus be calculated. One should note that the contribution of the electronic jitter introduced is neglected, as it is smaller than 50 ps.

Figure 12 shows this FWHM temporal response as a function of the detection efficiency (at 1550 nm) for an APD cooled at 223 K. One sees that an increase of the bias voltage—or equivalently of the detection efficiency—translates into a reduction of the temporal response. This response is typically around 300 ps at 10% efficiency (see inset) and can be as low as 150 ps for efficiencies around 20%. The inset of figure 12 represents the overall temporal response to the laser pulse at an excess bias voltage corresponding to a detection efficiency of 10%. The vertical scale is logarithmic. The falling edge features a slow tail, caused by photogenerated carrier diffusion. Variations of the width of the temporal response among APDs have been observed. Although the values shown in figure 12 are typical, some APDs have been found to exhibit a temporal response 50% longer. An optimization

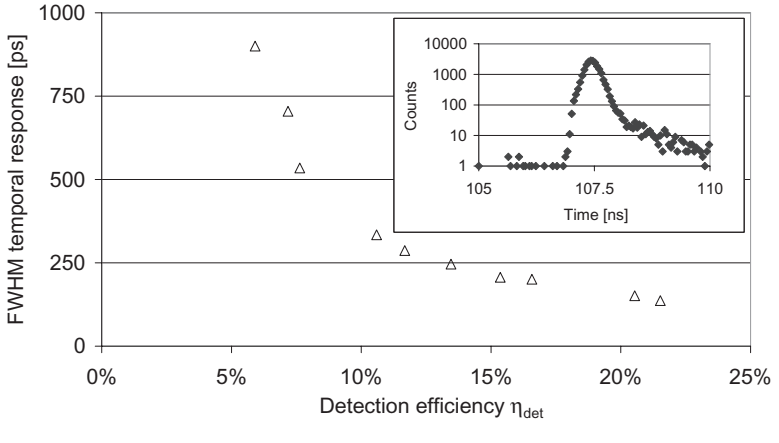


Figure 12. FWHM temporal response of the EPM 239 APD. Inset: response to a 120 ps FWHM pulse laser at an excess bias voltage corresponding to a detection efficiency of 10%.

of the structure of the APDs by their manufacturer could most certainly lead to improvements.

5. Applications

The field of applications of single-photon detection beyond 1 μm is very broad and constantly expanding. As an illustration, two applications—one in telecom instrumentation and the other one in quantum optics—are presented here.

5.1. *Telecom instrumentation*

Optical time-domain reflectometers (OTDRs) are very common tools used to characterize optical components and networks. A source emits light pulses coupled into a device under test. The amount of light reflected as a function of the time from the emission is then recorded. Knowledge of the index of refraction of the device under test allows one to convert this time into a distance. This principle makes it possible to perform distributed measurements of optical properties and to locate faults or bad connectors in optical fibre networks.

The use of a detector featuring the ability to detect single photons allows an improvement either of the dynamic range or of the spatial resolution, as well as a suppression of the dead-zone following an intense reflection. The first photon-counting OTDR measurements were reported by Healey as early as 1981 [11]. The group of Cova has also investigated this field [12]. Commercial photon-counting OTDRs are now available for various wavelengths [13, 14].

Figure 13 shows a schematic diagram of a photon-counting OTDR. It uses an APD operated in gated mode with 2 ns gates. The position of the gate is scanned to move the investigation zone along the device under test. In order to reduce the overall measurement time, trains of gates are used to probe multiple zones with a single laser pulse.

A typical figure of merit for conventional OTDRs is their dynamic range, as it essentially determines the maximum measurement distance. Figure 14 shows a series of three SMF fibres, connected by FC/PC connectors, of a total length of about 67 km. The first trace is a conventional OTDR measurement of the system, using a spatial resolution of 100 m (1 μs pulses). The second trace shows the same

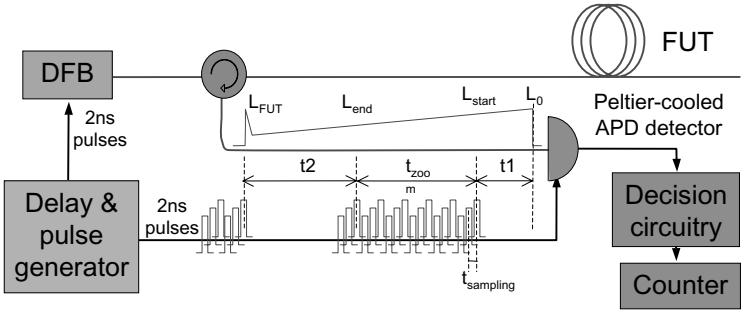


Figure 13. Schematic set-up of the photon-counting OTDR. DFB: distributed feedback laser, Var. att.: variable attenuator, Circ.: circulator, FUT: fibre under test. The use of trains of gates (comb of detection gates to gather information on several locations for each laser pulse) is also shown.

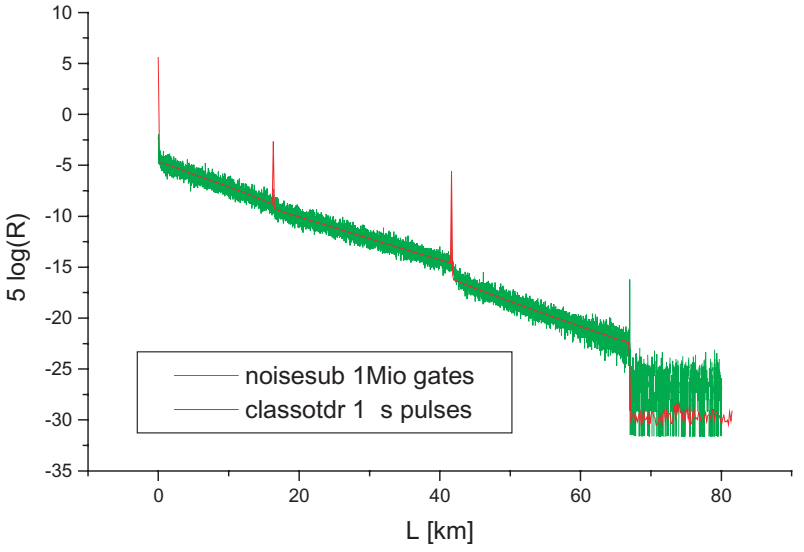


Figure 14. Measurement of a link consisting of three sections of single-mode fibre with a conventional OTDR and a photon-counting OTDR.

system measured with a photon-counting OTDR. In order to lower statistical noise, a large number (10.6) of gate openings is employed. Due to the low sampling resolution of 5 m, the reflective peak heights are not correctly reproduced as they do not necessarily fall within the 20 cm gate windows. The conventional and photon-counting OTDR traces agree to within 0.1 dB. As the figure demonstrates, the useful measurement distance for the present example roughly coincides with the system length (67 km), as afterwards signal and noise start to overlap. The corresponding dynamic range amounts thus to 20 dB.

As previously mentioned, one of the main advantages of a photon-counting OTDR is its superior spatial resolution. To illustrate this property, the measurement of an assembly of two connectors separated by a 15 cm patchcord is shown on figure 15. This length corresponds to the two-points resolution (according to 3 dB dip criteria). One can also see that this property does not depend on the position of the assembly, as it is identical if it is located at a distance of 3 m or 81 km of the OTDR output port. Indeed the two traces overlap perfectly (SNR is obviously reduced at 81 km). With a conventional OTDR, the resolution is typically several metres.

An important problem encountered with conventional OTDR is the presence of dead-zones after strongly reflective events leading to detector saturation. The photodetector indeed requires a certain time to recover full sensitivity again. With a photon-counting OTDR, the use of gates largely reduces this effect. The detector is indeed (almost) turned-off outside the gates. As discussed above in the section on afterpulses, the probability of detecting photons reaching the detector before the gate is not exactly zero, which can also cause a dead-zone effect. In the case of a Fresnel reflection ($R = -15$ dB) for example, it takes a time corresponding to about 5.5 km for the detector performance to reach its normal level again. This case is however not very typical of real networks. For non-saturating reflective events, which are more likely to be found on a real network, this effect can be

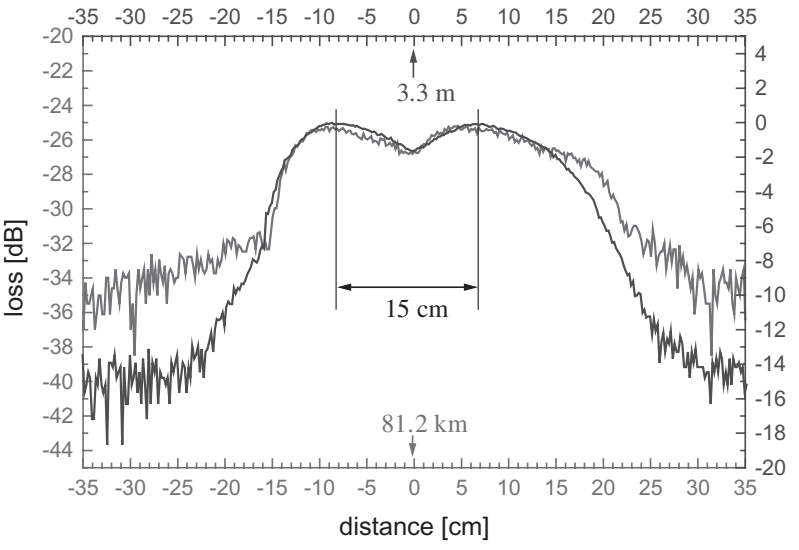


Figure 15. Measurement of the reflections of two FC/PC connectors separated by a 15 cm patchcord and located at a distance of 3.3 m (dark curve and axis) and 81.2 km (grey curve and axis).

completely neglected. One should also note that afterpulses can deteriorate the signal. It is however possible to mitigate this effect either by the use of a dead time or an algorithmic signal correction [15].

The photon-counting OTDR is a tool well suited for the survey of metropolitan area networks. A complete discussion of this application can be found in [16]. In practice, it may be beneficial to use a conventional OTDR for general measurements and the photon-counting one to perform zooms on zones that need further investigation.

It was also recently proposed to use a photon-counting OTDR to perform distributed measurements of the polarization properties of a fibre [15]. In this case, a polarization controller and an adjustable linear polarizer are placed between the circulator and the fibre under test of figure 13. One can take advantage of the spatial resolution of the photon-counting OTDR to measure the beat length of fibre sections, even in the case of high birefringence fibres. The detected signal exhibits oscillations with a period equal to half the beat length. This quantity can thus be extracted by calculating the Fourier transform of the signal in a certain window corresponding to a fibre section. This technique allows one to locate high polarization mode dispersion (PMD) fibre sections in a deployed network.

Optical time-domain reflectometry can also be used to perform distributed measurements in free-space. In this case, it is known as LIDAR. Instead of connecting an optical fibre to the output port of the system, one uses a telescope to produce a collimated beam. Initial experiments have been performed recently [17]. Spatial and temporal distributions of multi-layered structures of clouds were observed in the atmosphere up to an altitude of 4.5 km. Working with light at 1550 nm is advantageous, as this wavelength is considered as 'eye safe'.

Techniques taking advantage of the excellent temporal response and sensitivity of APDs in Geiger mode to measure the chromatic dispersion of optical fibres have also been developed [13].

5.2. *Quantum optics*

Detecting single-photons—the elementary quanta of light—is a key technology for quantum optics. Working at telecom wavelengths allows one to take table-top experiments and to perform them over long distances. Recent examples include long distance quantum teleportation [18] or demonstration of the Deutsch–Josza algorithm [19].

Quantum key distribution (QKD) [20] is probably the application of single-photon detection at telecom wavelength that currently triggers the strongest interest. It allows one to exchange a cryptographic key whose secrecy is guaranteed by the laws of quantum physics. The bits of the key are encoded on single photons, which are quantum systems. Their interception necessarily translates into perturbations. Eavesdropping can thus not go undetected.

When single photons are used to transport information between two stations connected by optical fibre, it is essential to minimize losses by channel attenuation. The wavelength of the photons must clearly be around 1550 nm, which means that one must rely on InGaAs APDs as single-photon detectors.

QKD is well suited to the use of APDs in the gated mode, as the time of arrival of the photons is known in most systems. For this application, a detector should ideally have a detection efficiency as high as possible and a dark count probability as small as possible. The effect of afterpulses can be mitigated by the use of a dead time, although this has an impact on the maximum counting rate. The two figures of merit of a QKD system are the raw key distribution rate R_{raw}:

$$R_{\mathrm{raw}} = \mu T_{\mathrm{L}} T_{\mathrm{R}} \eta_{\mathrm{det}} f_{\mathrm{rep}}. \tag{2}$$

In this equation, μ represents the average number of photons per pulse. Although this value should be optimized taking into account the transmission distance and the key distribution protocole, we will set it to 0.1 to gain some insight into order of magnitudes. T_{L} represents the probability for a photon to be transmitted through the optical fibre channel. We will assume that the optical fibre channel features an attenuation of $0.22\,\mathrm{dB\,km^{-1}}$, which is a typical value. T_{R} is the transmission probability of the receiver and can be set at 0.5. η_{det} is the detection efficiency of the detector and f_{rep} is the repetition frequency.

The second figure of merit is the so-called quantum bit error rate (QBER). With the assumption that afterpulses can be neglected, it can be expressed as

$$QBER = QBER_{\mathrm{opt}} + QBER_{\mathrm{det}}. \tag{3}$$

In this equation, $QBER_{\mathrm{opt}}$ is the error fraction coming from imperfect optical contrast in the set-up. It is typically of the order of 0.2% in the case of self-compensating QKD systems [18]. $QBER_{\mathrm{det}}$ represents the error fraction stemming from detector dark counts.

$$QBER_{\mathrm{det}} = p_{\mathrm{dc}}/(2p_{\mathrm{dc}} + \mu T_{\mathrm{L}} T_{\mathrm{R}} \eta_{\mathrm{det}}). \tag{4}$$

$QBER_{\mathrm{det}}$ increases with distance and limits the range of a QKD link. For the detector whose performance was presented above ($p_{\mathrm{dc}} = 10^{-5}$ and $\eta = 10\%$), it appears that a QBER of the order of 3% would be achieved after a distance of 100 km, which shows that QKD over such a range is possible. This means that the span of practical QKD systems is sufficient for the vast majority of metropolitan area network applications.

6. Conclusions

Gated mode operation of InGaAs/InP APDs enables single-photon detection at telecom wavelength. A quantum detection efficiency of 10% at 1550 nm and a dark count probability of $10^{-5}\,ns^{-1}$ are typical. The spectral sensitivity of these detectors spans the 1100–1650 nm wavelength interval. Presently, the major difficulty comes from afterpulses, which limit the maximum repetition rate. Temporal response of the order of 300 ps at a detection efficiency of 10% is typical. Future optimization of APD structure may certainly yield improvements on these characteristics.

These detectors can be used in optical time domain reflectometers. Compared to conventional OTDRs, single-photon detectors can improve the dynamic range by 20 dB or two-point resolution to 15 cm, while reducing dead-zone effects.

Another application of single-photon detection at telecommunication wavelength is quantum key distribution. From the performance presented here, it is clear that a range exceeding 100 km is possible.

References

[1] Lacaita, A., Francese, P. A., Zappa, F., and Cova, S., 1994, *Appl. Optics*, **33,** 6902.
[2] Gol'tsman, G. N., Okunev, O., Chulkova, G., Lipatov, A., Semenov, A., Smirnov, K., Voronov, B., and Dzardanov, A., 2001, *Appl. Phys. Lett.*, **79,** 705.
[3] Lacaita, A., Zappa, F., Cova, S., and Lovati, P., 1996, *Appl. Optics*, **35,** 2986.
[4] Ribordy, G., Gautier, J.-D., Zbinden, H., and Gisin, N., 1998, *Appl. Optics*, **37,** 2272.
[5] Rarity, J. G., Wall, T. E., Ridley, K. D., Owens, P. C. M., and Tapster, P. R., 2000, *Appl. Optics*, **39,** 6746.
[6] Hiskett, P. A., Buller, G. S., Loudon, A. Y., Smith, J. M., Gontijo, I., Walker, A. C., Townsend, P. D., and Robertson, M. J., 2000, *Appl. Optics*, **39,** 6818.
[7] www.idquantique.com
[8] Cova, S., Ghioni, M., Lacaita, A., Samori, C., and Zappa, F., 1996, *Appl. Optics*, **35,** 1956.
[9] Bethune, D. S., and Risk, W. P., 2000, *IEEE J. Quantum Electron.*, **36,** 340.
[10] Tomita, A., and Nakamura, K., 2002, *Opt. Lett.*, **27,** 1827.
[11] Healey, P., 1981, *Electron. Lett.*, **17,** 751.
[12] Lacaita, A., Francese, P. A., and Cova, S., 1993, *Opt. Lett.*, **18,** 1110.
[13] www.luciol.com
[14] www.opto-electronics.com
[15] Wegmuller, M., Scholder, F., and Gisin, N., 2003, *IEEE J. Lightwave Technol.*, submitted.
[16] Wegmuller, M., and Gisin, N., 2003, *Proceedings of the European Conference of Optical Communications*, accepted.
[17] Saito, Y., Yoshida, T., and Nomura, A., 2000, *Proceedings of the 20th International Laser Radar Conference*, 10–14 July, Vichy, France.
[18] Marcikic, I., de Riedmatten, H., Tittel, W., Zbinden, H., and Gisin, N., 2003, *Nature*, **421,** 509.
[19] Brainis, E., Lamoureux, L.-P., Cerf, N. J., Emplit, Ph., Haelterman, M., and Massar, S., 2003, *Phys. Rev. Lett.*, **90,** 157902-1.
[20] Gisin, N., Ribordy, G., Tittel, N., and Zbinden, H., 2002, *Rev. Mod. Phys.*, **74,** 145.

Towards practical and fast Quantum Cryptography

Nicolas Gisin[1], Grégoire Ribordy[2], Hugo Zbinden[1], Damien Stucki[1], Nicolas Brunner[1], Valerio Scarani[1]
[1] *Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland*
[2] *idQuantique, 3, Chemin de la Marbrerie, CH-1227 Carouge, Switzerland*
(September 28, 2005)

We present a new protocol for practical quantum cryptography, tailored for an implementation with weak coherent pulses. The key is obtained by a very simple time-of-arrival measurement on the *data line*; an interferometer is built on an additional *monitoring line*, allowing to monitor the presence of a spy (who would break coherence by her intervention). Against zero-error attacks (the analog of photon-number-splitting attacks), this protocol performs as well as standard protocols with strong reference pulses: the key rate decreases only as the transmission t of the quantum channel. We present also two attacks that introduce errors on the monitoring line: the intercept-resend, and a coherent attack on two subsequent pulses. Finally, we sketch several possible variations of this protocol.

I. INTRODUCTION

Quantum cryptography [1], or quantum key distribution (QKD), is probably the most mature field in quantum information, both in theoretical and in experimental advances. On the theoretical side, almost all QKD protocols have been proven to provide unconditional security in some regime; on the practical side, QKD has already reached the stage of commercial prototypes. Still, much work is needed. A big task consists in bringing both theory and applications in contact again: practical QKD systems do not fulfill all the requirements of unconditional security proofs (or, if you prefer, these proofs are still too abstract to cope with a practical system). Here, we address a different question: we aim for the *most practical* QKD system. Instead of looking for a new implementations of known protocols, we choose to start from scratch by inventing a new protocol. There are two basic requirements:

- The protocol must be easily implementable, say with the smallest number of standard telecom devices. Note that this requirement, as a side benefit, may simplify security studies: we have learnt in the recent years that any optical component can be regarded as a "Trojan horse" because of its imperfections [2].
- The security of the system must be guaranteed by quantum physics, thence in some way quantum coherence must play a role.

The goal of this paper is to illustrate this program by presenting such a system. the key is created in a *data line* that is probably the simplest one can think of — just measure the time of arrival of weak pulses. The intervention of a spy is checked interferometrically in a *monitoring line*. In Section II, we define precisely the protocol and stress its advantages. In Section III, we present a quantitative study of security. Finally, Section IV presents a number of possible variations on the main idea.

II. THE PROTOCOL

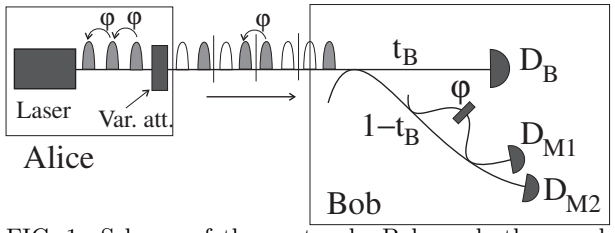


FIG. 1. Scheme of the protocol. Bob reads the raw key in detector D_B, the monitoring line checks for the breaking of quantum coherence due to an eavesdropper. See text for details

A. The source

Alice uses a mode-locked laser, producing pulses of mean photon-number μ that are separated by a fixed and well-defined time τ; with a variable attenuator, she can blocks some of the pulses (note that a more economical source would just consist of a cw laser followed by the variable attenuator). Each logical bit is encoded in a two-pulse sequence according to the following rules:

$$|0_A\rangle = \left|\sqrt{\mu}\, e^{i(2k-1)\varphi}\right\rangle_{2k-1} |0\rangle_{2k}\,, \tag{1}$$

$$|1_A\rangle = |0\rangle_{2k-1} \left|\sqrt{\mu}\, e^{i\,(2k)\varphi}\right\rangle_{2k}\,. \tag{2}$$

For instance, the eight-pulse sequence drawn in Fig. 1 codes for the four-bit string 0100 (read in temporal order, that is, from right to left). For small μ, the states $|0_A\rangle$ and $|1_A\rangle$ have a large overlap because of their vacuum component. Since the laser is mode-locked, there is a phase coherence between any two non-empty pulses.

Leaving a more general discussion for Section IV, we focus on the case where bit number k is 1 and bit number $k+1$ is 0, like bits number 2 and 3 of 1. Then *across the bit-separation* there is a phase coherence:

$$\left|\sqrt{\mu}\, e^{i(2k)\varphi}\right\rangle_{2k} \left|\sqrt{\mu}\, e^{i(2k+1)\varphi}\right\rangle_{2k+1}. \tag{3}$$

Note that the choice of the value of φ is arbitrary, so from now on we set $\varphi = 0$.

B. The "data line"

The pulses now propagate to Bob, on a quantum channel characterized by a transmission $t = 10^{-\alpha\, d/10}$ (a typical value for α in optical fibers is 0.2 dB/km). Bob's setup first splits the pulses using a non-equilibrated beam-splitter with transmission coefficient t_B. The pulses that are transmitted are used to establish the raw key (*data line*). To obtain the bit value, Bob has to distinguish unambiguously between the two non-orthogonal states

$$|0_B\rangle = |\alpha\rangle_{2k-1}|0\rangle_{2k}, \tag{4}$$

$$|1_B\rangle = |0\rangle_{2k-1}|\alpha\rangle_{2k} \tag{5}$$

with $\alpha = \sqrt{\mu\, t\, t_B}$ — we have omitted the phase due to the free propagation, which is the same for all pulses. As well-known, unambiguous discrimination between two pure states can succeed with probability $p_{ok} = 1 - |\langle 0_B|1_B\rangle|$; in the present case, the overlap is $|\langle 0_B|1_B\rangle| = e^{-|\alpha|^2}$, and consequently $p_{ok} = 1 - e^{-\mu\, t\, t_B}$. Now, there is an obvious way to achieve this result: photon counting with a perfect detector, because p_{ok} is just the probability that the detector will detect something. The realistic situation where the detector has a finite efficiency η can be modelled by an additional beam-splitter with transmittivity η followed by a perfect detector; in this case, η appears in the exponent as well. In conclusion, the optimal unambiguous discrimination between $|0_B\rangle$ and $|1_B\rangle$ is achieved by the most elementary strategy, simply try to detect where the photons are. Later, Bob must announce Alice which items he has detected: this is how Alice and Bob establish their raw key. Note that no error is expected on this line, if the switch is perfect and in the absence of dark counts of the detector: a bit-flip is impossible because it would correspond to a photon jumping from a time-bin to another.

Note that the simplicity of Bob's data line has concrete practical advantages. There are no lossy and active elements. Hence, the transmission range can be increased and no random number generator is needed.

As for the data line, our protocol is similar to the one of Debuisschert and Boucher [3]. However there, the security was obtained by the overlap in time between the pulses coding for different bits. Here, we use rather the monitoring line described in the next paragraph.

C. The "monitoring line"

The pulses that are reflected at Bob's beam-splitter go to an interferometer that is used for monitoring Eve's presence (*monitoring line*). Here is where quantum coherence plays a role. Let α_j be the amplitude of pulse j entering the interferometer: in particular, $|\alpha_j|^2$ is either 0 or $\mu\, t\,(1 - t_B)$; and if both α_j and α_{j+1} are non-zero, then $\alpha_{j+1} = \alpha_j$. After the interferometer, the pulses that reach the detectors at time $j+1$ is given by

$$|D_{M1}\rangle = \left|i\tfrac{\alpha_j + \alpha_{j+1}}{2}\right\rangle \tag{6}$$

$$|D_{M2}\rangle = \left|\tfrac{-\alpha_j + \alpha_{j+1}}{2}\right\rangle. \tag{7}$$

Now, if either α_j or α_{j+1} are zero, then $|D_{M1}|^2 = |D_{M2}|^2 = \frac{1}{2}\mu\, t\,(1 - t_B)$; i.e., conditioned to the fact that a photon takes the monitoring line, the probabilities of detecting it in either detector is $\frac{1}{2}$. However, if both α_j and α_{j+1} are non-zero, then $|D_{M1}|^2 = \mu\, t\,(1 - t_B)$ and $|D_{M2}|^2 = 0$: only detector D_{M1} can fire. Consider then again the case where bit number k is 1 and bit number $k+1$ is 0: as we said above, in this case the two consecutive pulses $2k$ and $2k+1$ are non-empty. This means that, *if coherence is not broken*, detector D_{M2} cannot fire at time $2k+1$. If Eve happens to break the coherence by reading the channel, it could be detected this way.

Actually, it turns out that, as just described, the protocol is insecure: Eve can make a *coherent* measurement of the number of photons in the two pulses across the bit-separation. With such an attack, she would not break the coherence, thus introduce no errors in the monitoring line, and obtain almost full information (see next Section for more details). There are several ways of countering this attack: here, we make use of *decoy sequences*, inspired by the idea of "decoy states" introduced by Hwang [4] and by Lo and co-workers [5], but different in its implementation. The principle is the following: with probability f, Alice leaves both the $(2k-1)$-th and the $2k$-th pulses non-empty. A decoy sequence does not encode a bit value (in contrast to the decoy states of [4,5] that still encode a state, but in a different way): thence, if the item is detected in the data line, it will be discarded in public discussion. However, if a detection takes place in the monitoring line at time $2k$, then it must be in detector D_{1M} because of coherence. Now Eve can no longer pass unnoticed: if she attacks coherently across the bit separation, then she breaks the coherence of the decoy sequences; if she attacks coherently within each bit, then she breaks the coherence across the separation; finally, if she makes a coherent attack on a larger number of pulses, then she breaks the coherence in fewer positions but gets much less information.

Thus, errors are rare: they appear only in the monitoring line, and just for a fraction of the whole cases. Still, one can estimate the error (thence, the coherence of the channel) in a reasonable time, if the bit rate is high.

D. Summary of the protocol

Let's summarize the protocol before moving to a more quantitative study of security:

1. Alice prepares "bit 0" with probability $\frac{1-f}{2}$, "bit 1" with probability $\frac{1-f}{2}$ and the decoy sequence with probability f. This is repeated a large number of times.

2. At the end of the exchange, Alice reveals the items $\{k_d\}$ corresponding to a decoy sequence. Bob removes all the detections at times $2k_d - 1$ and $2k_d$ from his raw key, and he looks whether detector D_{2M} has ever fired at times $2k_d$. This way, Alice and Bob estimate the break of coherence of decoy pulses.

3. On the remaining fraction of sent bits $1 - f$, Bob reveals the times $2k + 1$ in which he had a detection in D_{2M}. Alice verifies if some of these items correspond to a bit sequence "1,0"; thus, Alice and Bob estimate the break of coherence across the bit-separation.

4. Finally, Bob reveals the items that he has detected in the data line. Alice and Bob run error correction and privacy amplification on these bits and end up with a secret key.

Should one say in one sentence where the improvement lies, here it is: *one can define a very simple data line and protect it quantum-mechanically.*

At this point, two important remarks can be done. First, this protocol cannot be analyzed in terms of qubits. This is obvious, because any bits and coherence are checked on differently defined pairs. In particular, there is not a "natural" single-photon version of the protocol (simply replace non-empty coherent state with one-photon Fock states would be dramatic, since all the sequences would become orthogonal). The second remark is the answer to a possible question. With the idea of a simple data line for key creation, and a "complementary" line for monitoring, one may implement a version of the BB84 protocol: Alice and Bob agree to produce the key using only the Z basis; sometimes Alice prepares one of the eigenstates of the X basis that acts as a decoy state. Which are the advantages of our protocol? We are going to see that our protocol is much more robust against attacks at zero errors (the analog of photon-number-splitting attacks).

III. QUANTITATIVE ANALYSIS OF SECURITY

For a reasonable comparison with experiment, we must introduce the following parameters

- The visibility V of the monitoring interferometer, whence the probability that D_{2M} fires in a time corresponding to a coherence is $\frac{1-V}{2}$ instead of zero. We suppose that Eve can take advantage of these imperfections: for instance, if the reduced visibility is due to $\varphi \neq 0$ in the interferometer, Eve can systematically correct for this error by displacing the pulses, and then reproduce V by adding errors in a way that is profitable for her.

- The imperfections of the three Bob's detectors, supposed to be identical for simplicity: the quantum efficiency η and the probability per gate of a dark count p_d. Typical values are $\eta = 10\%$, $p_d = 10^{-5}$. These imperfections are not given to Eve (see Section IV on the possibility that Eve forces a detection, thus effectively setting $\eta = 1$ for some pulses).

For simplicity in writing, we make all the quantitative analysis in the limit of small mean photon-number in Bob's channel, that is $\mu t << 1$.

A. Parameters Alice-Bob on the data line

First, we compute the parameters of Alice-Bob on the data line. Bob's detection rate in D_B, once decoy sequences are removed, is

$$R_B = \left[\mu T + (1 - \mu T)p_d\right](1 - f) \tag{8}$$

where $T = t\, t_B\, \eta$. In other words, R_B times the number of two-pulse sequences sent by Alice is the length of the raw key.

If we assume that the switch prepares really empty pulses when it is closed, the error expected in this line is only due to the dark counts of the detectors:

$$Q = \frac{\frac{1}{2}(1 - \mu T)p_d(1 - f)}{R_B} \tag{9}$$

because dark counts may make the detector fire at both times with equal probability. The mutual information Alice-Bob in bits per sent photon is thence

$$I(A : B) = R_B \left[1 - H(Q)\right]. \tag{10}$$

In what follows, we shall concentrate on attacks by Eve that do not modify Q. Before moving to that, let's have a look at the monitoring line as well.

B. About the monitoring line

In the presence of dark counts and reduced visibility, the meaningful detection probabilities in D_{M1} and D_{M2}, neglecting double counts are the following [6]:

$$\text{Time } 2k\text{, decoy seq. } : \; R^d_{1,2} \;=\; R^d_{M1,2}\, f \tag{11}$$

$$\text{Time } 2k+1\text{, seq. "1,0" } : \; R^{10}_{1,2} \;=\; R^{10}_{M1,2}\, \frac{1-f}{4} \tag{12}$$

where, denoting $\tilde{T} = t\,(1-t_B)\,\eta$, we have defined

$$R^x_{M1,2} = \mu\tilde{T}\frac{1 \pm V_x}{2} + \left(1 - \mu\tilde{T}\frac{1 \pm V_x}{2}\right) p_d\,. \tag{13}$$

Contrary to the errors due to dark counts, the departure from perfect visibility will be entirely attributed to Eve. This is why we consider *a priori* different values V_d and V_{10} for the visibility in the two cases: as we shall see, Eve's attacks may be different.

C. Eve's attacks

If Bob's detector has dark counts, $I(B:E)$ is smaller than $I(A:E)$ for a prepare-and-measure scheme, because even if Eve knows perfectly what Alice has sent, she cannot know whether Bob has detected a photon or has had a dark count. Thus in our case, the Csiszar-Körner bound [7] that gives an estimate of the extractable secret key rate becomes

$$\begin{aligned} R \geq I(A:B) \;-\; &\min\big\{I(A:E), I(B:E)\big\} \\ &= I(A:B) \;-\; I(B:E)\,. \end{aligned} \tag{14}$$

Therefore, we have to compute the mutual information Bob-Eve.

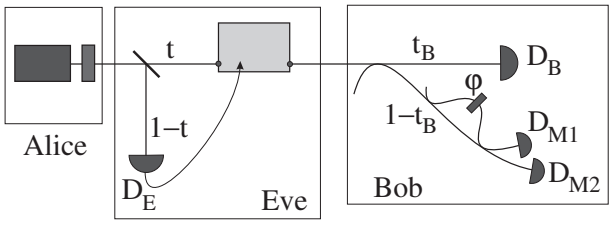


FIG. 2. Scheme with Eve.

The kind of attacks by Eve that we consider is sketched in Fig. 2. We can give Eve all the losses in the line, that is, we can suppose that Eve removes a fraction $1-t$ of the photons, and forwards the remaining fraction t to Bob on a lossless line. We are going to study:

- An attack in which Eve can gain information without introducing errors. This is related to the losses on the line; it is the analog of the usual photon-number-splitting attack [8,9], but is a different attack and less powerful.
- Eve can immediately know if the previous attack was successful or not; in the case it wasn't, we consider further the possibility of attacks that introduce errors in the monitoring line (but still no errors in the data line). Specifically, we study a usual intercept-resend strategy, and a more clever attack which is performed coherently on two subsequent pulses across the bit-separation.

1. Eve's attack without errors

In the case of BB84 and many other protocols, Eve can exploit multi-photon pulses in a lossy line to perform the *photon-number-splitting attack* [8,9]: she counts the photons in each pulse, and whenever this number is larger than one, she keeps one photon in a quantum memory and forwards the remaining photons to Bob on a lossless line. As such, this attack is not error-free in the present protocol: counting the photons in each pulse breaks the coherence between successive pulses, thus introducing errors in the monitoring line — actually, because of the peculiar encoding of the bits, this attack reduces here to the intercept-resend, see below.

More subtle is the analysis of a practical version of the attack using *cascaded beam-splitters* [10]: Eve uses a highly unbalanced BS, with transmission $1-\varepsilon$ and reflection ε; if she has a detection, she forwards the remaining photons to Bob; otherwise, she begins anew, and so on until the losses that she introduces reach the transmission t of the quantum channel. The advantage of this strategy is that, in the presence of two or more photons, it is very rare that more than one photon is coupled into Eve's detector. Indeed, this beam-splitting attack approximates a photon-counting. In our case, this strategy will introduce errors in the monitoring line as well: it does not modify the relative phase, but the relative intensity between subsequent pulses, thus leading to an unbalancing of the interferometer. The full analysis of such a strategy will be studied in a further work.

In summary, both the ideal photon-number-splitting and its approximate implementation through cascaded beam-splitters do not rank among the zero-error attacks against our protocol. In fact, Eve can only perform the basic *beam-splitting attack*: she removes a fraction $1-t$ of the photons, and transmits the remaining fraction t to Bob on a lossless line. With the fraction that she has kept, the best thing Eve can do is just to measure them (recall the argument about optimal unambiguous state discrimination). This way, she detects $\mu(1-t)$ photons per pulse. When Eve has a detection in D_E, she knows the bit that Alice has sent. Then she lets the remaining part of the pulse travel to Bob on the lossless line

(the grey box of Fig. 2 is simply a line). Bob detects something exactly as if Eve had not been there. So

$$I(B:E|D_E) = I(A:B)\,. \tag{15}$$

In summary, Eve knows a fraction $\mu(1-t)$ of the key just because of the losses in the quantum channel: this fraction must always be subtracted in privacy amplification.

It is instructive to compute the optimal value of μ under the assumption that Eve introduces no errors, and neglecting dark counts ($Q = 0$). In BB84, this value is $\mu_{BB84} = t$, giving $R_{BB84} = \frac{1}{4}\eta\, t^2$ [11]. Here, Alice and Bob must maximize R given in (14); using (10) and (15), this reads

$$R = \mu\, t\, t_B\, \eta\, (1-f)\, \big(1-\mu(1-t)\big)\,. \tag{16}$$

The optimization $dR/d\mu = 0$ is readily done and yields

$$\mu_{opt} = \frac{1}{2(1-t)} \tag{17}$$

whence

$$R_{opt} = \frac{1}{4(1-t)}\, t\, t_B\, \eta\, (1-f)\,. \tag{18}$$

This is an important improvement over BB84: μ_{opt} is large and is basically constant with decreasing t (long quantum channels); as a consequence, the secret-key rate decreases only *linearly* (and not quadratically) with t. This is the same improvement that can be obtained by using decoy states [5] or a strong reference pulse [12]; note however that the hardware is much simpler here.

When Eve's detector D_E does not fire, which happens with probability $1-\mu(1-t)$, Eve must perform some attack on the pulses flying to Bob if she wants to gain some information. These attacks will certainly introduce errors, either in the data line or in the monitoring line. In the following, we present two such attacks (Fig. 3): a basic intercept-resend (I-R), and a photon-number-counting attack performed coherently on two subsequent pulses across the bit-separation (2c-PNC).

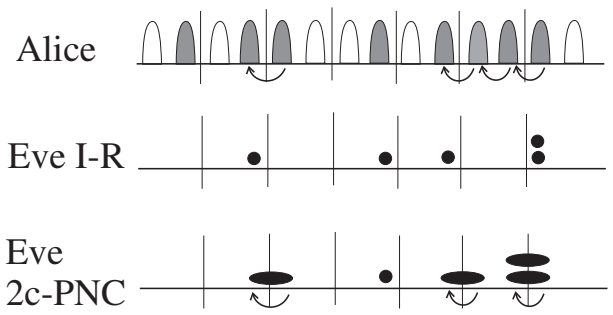


FIG. 3. Comparison of two attacks that introduce errors. In the I-R attack, Eve prepares a sequence of localized Fock states, thus breaking the coherence everywhere. In the 2c-PNC attack, Eve prepares a sequence of Fock states that are delocalized across the separation of bits: only the coherence of decoy sequences is broken. Note that arrows denote only coherence between subsequent pulses, the one checked by the interferometer; however, on the original sequence, all the non-empty pulses are coherent with one another, while in the sequences after Eve's attack only the indicated coherence remains.

2. Eve's attack with errors (I): intercept-resend

Let's begin with the intercept-resend (I-R) strategy. Eve simply detects the pulse flying to Bob: her detector will fire with probability μt, and in this case she prepares a *single-photon* in the good time-bin and forwards it to Bob. Obviously, both R_B and Q are unchanged under this strategy.

Note that R_B will be the sum of three terms: Eve has detected and Bob detects too; Eve has detected and Bob has a dark count; Eve has not detected and Bob has a dark count. Now, Eve can distinguish the last one from the two first, and she knows that in the last case she has no information on Alice's and Bob's bits. So

$$I(B:E|IR) = [R_B - (1-\mu t)p_d(1-f)]\big[1-H(Q')\big] \tag{19}$$

where

$$Q' = \frac{\frac{1}{2}(1-t_B\eta)p_d}{t_B\eta + (1-t_B\eta)p_d} \tag{20}$$

is the fraction of Bob's detection on which she has the wrong result.

Of course, the I-R attack breaks all the coherences (see Fig. 3), and will therefore introduce errors in the monitoring line. Specifically, whenever Eve has performed the I-R attack,

$$V_{d|IR} = V_{10|IR} = 0\,. \tag{21}$$

3. Eve's attack with errors (II): 2-coherent PNC

In the absence of decoy sequences, Eve may obtain information without introducing errors in the monitoring line, by counting the number of photons coherently between two pulses, not within each bit but across the separation line (see Fig. 3). This attack does not break the phase between these pulses. Of course, if Eve finds $n > 0$ photons, on the spot she does not know to which bit the photon belongs; but she will learn it later, by listening to Bob's list of accepted bits [13]. Actually, in some very rare case Eve still does not get any information: if Eve

prepares $n > 0$ photons in two successive two-pulse sequences, and Bob accepts a detection in the bit common to both sequences, Eve has no idea of his result. However, since such cases are rare, we make the conservative assumption that Eve always gets full information. Thus

$$I(B:E|2cPNC) = I(B:E|IR)\,. \tag{22}$$

Eve has introduced errors in the monitoring line *only* in the items corresponding to decoy sequences:

$$V_{d|2c} = 0\,,\; V_{10|2c} = 1\,. \tag{23}$$

4. Collecting everything

We can now collect all that we know form this analysis of security. The parameters describing Alice and Bob are those listed in paragraph III A above. Let p_{IR} and p_{2c} be the probabilities that Eve performs the I-R attack, resp. the 2c-PNC attack. Recall that she performs these attacks only when her detector D_E did not fire, so $p_{IR} + p_{2c} \leq 1 - \mu(1-t)$. Then:

$$\begin{aligned} I(B:E) = {} & \mu(1-t)\, R_B \left[1 - H(Q)\right] + \\ & + (p_{IR} + p_{2c})\, R'_B \left[1 - H(Q')\right] \end{aligned} \tag{24}$$

with the notation $R'_B = R_B - (1-\mu t)p_d(1-f)$ and with Q' given in (20). This is the expression that must be inserted into (14) to obtain the extractable secret key rate (in other terms, this is the quantity to be corrected by privacy amplification).

On the monitoring line, Alice and Bob measure (11) and (12), whence they extract V_d and V_{10} that inform them about Eve's attacks according to

$$V_d = 1 - p_{IR} - p_{2c}\,, \tag{25}$$

$$V_{10} = 1 - p_{IR}\,. \tag{26}$$

Note in particular that, if Alice and Bob find $V_d = V_{10}$, they can conclude that Eve has not used the 2c-PNC attack — by the way, this is why we presented the analysis of the I-R strategy, obviously worse than 2c-PNC from Eve's standpoint: in a practical experiment, $V_d = V_{10}$ is very likely to hold (after all, Eve is not there...). Therefore, formulae for the I-R attack will be useful in the analysis of experimental data.

IV. VARIATIONS AND OPEN QUESTIONS

A. Variations

Here are a few ideas of variations in the protocol, that may have some additional benefit and require further study:

- Alice may change during the protocol the definition of the pulses that define a bit. If there is a convenient fraction of decoy sequences, Eve has no way of distinguishing a priori which pairs of successive pulses encode a bit. This way, the effect of the 2c-PNC attack becomes equally distributed among decoy and "1,0" sequences, i.e. $V_d = V_{10} = 1 - p_{IR} - \frac{1}{2}p_{2c}$. Moreover, whenever Eve attacks the bit instead of attacking across the bit-separation, she cannot gain any information.

- In fact, nothing forces to define bits by subsequent pulses: Alice and Bob can decide later, adding a sort of "sifting" phase to the protocol. This means that Alice can now send whatever pulse sequence, she is no longer restricted to those that define a bit or a decoy sequence. It is not clear whether this modification helps, if the hardware is kept unchanged: Alice and Bob still check only the coherence between subsequent pulses; moreover, sifting means additional losses and additional information revealed publicly.

- Instead of introducing decoy sequences as we did above, one may study the effect of decoy pulses with different intensities, as proposed by Hwang and by Lo and co-workers to protect the BB84 protocol against the photon-number-splitting attack [4,5].

B. Possible loopholes

The difficulty in assessing the security of practical QKD, is the huge number of imperfections that may hide loopholes for security. These imperfections exist in all implementations and for all protocols, but their effect and the corresponding protection may vary. Here we present some of these.

- About Trojan-horse and similar realistic attacks [2]: Alice's setup must be protected against Trojan-horse attacks, with the suitable filters, isolators etc. In Bob's setup nothing is variable; however, one must prevent the possible light emission from avalanche photodiodes to become available to Eve: if the firing of a detector can be seen from outside Bob, the protocol becomes immediately insecure.

- After a detection, Bob's detectors are blind during some time. In particular, if Eve happens to know when Bob's detector D_{M2} has fired, she can attack strongly the subsequent pulses because no error will be detected then, and gain one bit (just one, because when D_B has fired, then it has a dead time as well). For the security of the protocol, Eve must have no way of assessing the firing of a detector,

and Bob must announce publicly this information only after the detector is ready again. This may imply some suitable synchronization in the software, or more simply, to shut D_B as long as D_{M2} has not recovered. The nuisance depends of course on the ratio between the raw bit rate and the dead time.

- In all this paper, we have considered only the case where Eve does not change Bob's detection rates in the data line and in the monitoring line. By sending out stronger pulses, Eve might force the detection of those items on which she has full information; but in turn, she would increase the rate of double counts among Bob's detectors. This effect must be quantified, and the number of double, or even triple, counts must be monitored during the experiment.

V. CONCLUSION

In conclusion, we have presented a new protocol for quantum cryptography whose realization is much simpler than that of previously described ones. Specifically, Bob's station is such that losses are minimized and no dynamical component is needed.

We thank H.-K. Lo for stimulating comments. We acknowledge financial support from idQuantique and from the Swiss NCCR "Quantum photonics".

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)

[2] A. Vakhitov, V. Makarov, D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001); V. Makarov, D. R. Hjelme, J. Mod. Opt. (to be published, 2004).

[3] T. Debuisschert, W. Boucher, Phys. Rev. A **70**, 042306 (2004)

[4] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003)

[5] H.-K. Lo, X. Ma, K. Chen, quant-ph/0411004

[6] Just to verify normalization, we notice that the rate of uninteresting detections are: for detection at time $2k+1$ corresponding to both sequences "0,0" and "1,1", $\left[\frac{\mu}{2}\tilde{T}\frac{1}{2}+\left(1-\frac{\mu}{2}\tilde{T}\frac{1}{2}\right)p_d\right]\frac{1-f}{4}$ in each detector; for detection at time $2k+1$ corresponding to sequence "0,1", $p_d\frac{1-f}{4}$ in each detector. Thus, the sum of all detections of non-decoy sequences sums up to $[\frac{\mu}{2}\tilde{T}+(2-\frac{\mu}{2}\tilde{T})p_d](1-f)$ as it should, because in average there are $\frac{\mu}{2}\tilde{T}$ photons at each time in non-decoy sequences and there are two detectors in which a dark count may happen.

[7] I. Csiszár, J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978)

[8] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000)

[9] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000)

[10] S. Félix, N. Gisin, A. Stefanov, H. Zbinden, J. Mod. Opt. **48**, 2009 (2001)

[11] A. Niederberger, V. Scarani, N. Gisin, quant-ph/0408122. Recall that we have assumed that the errors in the detectors are not given to Eve. In the most conservative case where all the errors are given to Eve, the estimates of μ must be multiplied by η [9].

[12] A. Acín, N. Gisin, V. Scarani, Phys. Rev. A **69**, 012309 (2004); M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004)

[13] For simplicity, we consider the case where Eve applies this attack on several consecutive items, see Fig. 3. One might as well consider the case where Eve applies the attack, sometimes, on just a single item. In this case, she learns full information (apart from dark counts) if she detects 0 photons and Bob accepts one of the two bits; while she does not learn anything if she has detected some photons and Bob accepts. The full analysis is longer than the one presented, and leads to the same yield in terms of information.

Fast and simple one-way quantum key distribution

Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden
Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland

(Received 17 June 2005; accepted 15 September 2005; published online 2 November 2005)

We present and demonstrate a new protocol for practical quantum cryptography, tailored for an implementation with weak coherent pulses to obtain a high key generation rate. The key is obtained by a simple time-of-arrival measurement on the *dataline*; the presence of an eavesdropper is checked by an interferometer on an additional *monitoring line*. The setup is experimentally simple; moreover, it is tolerant to reduced interference visibility and to photon number splitting attacks, thus featuring a high efficiency in terms of distilled secret bit per qubit. © *2005 American Institute of Physics*. [DOI: 10.1063/1.2126792]

Quantum key distribution (QKD) is the only method to distribute a secret key between two distant authorized partners, Alice and Bob, whose security is based on the laws of physics.[1] QKD is the most mature field in quantum information; nevertheless, there is still some work ahead in order to build a practical system that is reliable and at a same time fast and provably secure. In this paper we present an important improvement in this direction. The quest for *rapidity* is the inspiring motivation of this system: the idea is to obtain the secret bits from the simplest possible measurement (here, the time of arrival of a pulse) without introducing lossy optical elements at Bob's. *Security* is obtained by occasionally checking quantum coherence: in QKD, a decrease of coherence is attributed to the presence of the eavesdropper Eve, who has attacked the line and obtained some information on the bit values, at the price of introducing errors. *Reliability* is achieved by using standard telecom components; in particular, the source is an attenuated laser, and bits are encoded in time bins, robust against polarization effects in fibers. In this paper, we first define the protocol and demonstrate its advantages: simplicity, and robustness against both reduced interference visibility and photon number splitting (PNS) attacks.[2] Then, we present a first proof-of-principle experiment.

To date, the most developed setups for practical QKD implement the Bennett-Brassard 1984 (BB84) protocol[3] using phase encoding between two time bins, as sketched in the top of Fig. 1 (see Ref. 1 for a detailed description). The four states belonging to two mutually orthogonal bases are the $|1\rangle|0\rangle+e^{i\alpha}|0\rangle|1\rangle$, where $\alpha=0,\pi$ (bits 0 and 1 in the X basis) or $\alpha=\pi/2,3\pi/2$ (bits 0 and 1 in the Y basis). Bob detects in the X (Y) basis by setting $\beta=0$ ($\beta=\pi/2$). Both bases correspond thus to an interferometric measurement. As a first step toward simplicity, we replace (say) the Y basis with the Z basis $\{|1\rangle|0\rangle, |0\rangle|1\rangle\}$. Measuring in this basis amounts simply to the measurement of a time of arrival, and is thus insensitive to optical errors.[4] Bits are encoded in the Z basis, which can be used most of the time, the X basis being used only occasionally to check coherence.[5]

In a practical QKD setup, the source is an attenuated laser: here, Alice's source consists of a cw laser followed by an intensity modulator (IM), which either prepares a pulse of mean photon number μ or blocks completely the beam (empty or "vacuum" pulses).[9] The kth logical bit is encoded in the two-pulse sequences consisting of a nonempty and an empty pulse:

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k}, \tag{1}$$

$$|1_k\rangle = |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}. \tag{2}$$

Note that $|0_k\rangle$ and $|1_k\rangle$ are not orthogonal, due to their vacuum component; however, a time-of-arrival measurement, whenever conclusive, provides the optimal unambiguous determination of the bit value.[6] To check coherence, we produce a fraction $f \ll 1$ of *decoy sequences* $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$; while for BB84, one should produce the two states $|\sqrt{\mu/2}\rangle_{2k-1}|\pm\sqrt{\mu/2}\rangle_{2k}$. Now, due to the coherence of the laser, there is a well-defined phase between any two nonempty pulses: within each decoy sequence, but also *across the bit-separation* in the case where bit number k is 1 and bit number $k+1$ is 0 (a "1–0 bit sequence"). Since we produce equally spaced pulses, the coherence of both decoy and 1–0 bit sequences can be checked with a single interferometer (see Fig. 1, bottom). And there is a further benefit: coherence being distributed both within and across the bit separations, Eve cannot count the number of photons in any finite number of pulses without introducing errors:[6] in our scheme the PNS attacks can be detected.[7] To detect PNS attacks in BB84, one needs to complicate the protocol by the technique of decoy states, which consists of varying μ.[8]

The pulses propagate to Bob on a quantum channel characterized by a transmission t, and are split at a nonequilibrated beamsplitter with transmission coefficient $t_B \lesssim 1$. The pulses that are transmitted (*dataline*) are used to establish the

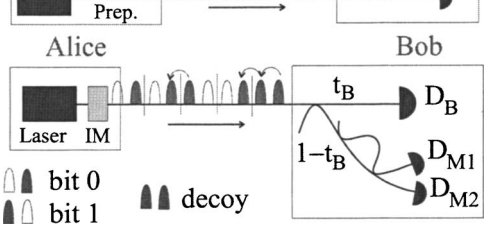


FIG. 1. A comparison of the currently implemented BB84 protocol with phase encoding (top) with the scheme proposed here (bottom). Arrows over pulses indicate coherence (the phase is set to 0 in our scheme).

raw key by measuring the arrival times of the photons. The counting rate is $R=1-e^{-\mu t t_B \eta}\approx \mu t t_B \eta$, where η is the quantum efficiency of the photon counter. The pulses that are reflected at Bob's beamsplitter go to the interferometer that is used to check quantum coherence (*monitoring line*). Indeed, when both pulses j and $j+1$ are nonempty, then only detector D_{M1} can fire at time $j+1$. Coherence can be quantified by Alice and Bob through the visibility of the interference,

$$V=\frac{p(D_{M1})-p(D_{M2})}{p(D_{M1})+p(D_{M2})}, \tag{3}$$

where $p(D_{Mj})$ is the probability that detector D_{Mj} fired at a time where only D_{M1} should have fired. These probabilities are small, the average detection rate on the monitoring line being $\frac{1}{2}\mu t(1-t_B)\eta$ per pulse. Still, if the bit rate is high, meaningful estimates can be done in a reasonable time.

Let's summarize the protocol.

(1) Alice sends a large number of times "bit 0" with probability $(1-f)/2$, "bit 1" with probability $(1-f)/2$ and the decoy sequence with probability f.
(2) At the end of the exchange, Bob reveals for which bits he obtained detections in the dataline and when detector D_{2M} has fired.
(3) Alice tells Bob which bits he has to remove from his raw key, since they are due to detections of decoy sequences (sifting).
(4) Analyzing the detections in D_{2M}, Alice estimates the break of coherence through the visibilities V_{1-0} and V_d associated, respectively, with $1-0$ bit sequences and to decoy sequences, and computes Eve's information.
(5) Finally, Alice and Bob run an error correction and a privacy amplification and end up with a secret key.

The performance of a QKD protocol is quantified by the achievable secret key rate R_{sk}. To compute this quantity, we need to introduce several parameters. The fraction of bits kept after sifting (sifted key rate) is $R_s(\mu)=[R+2p_d(1-R)]p_s$, with $R=\mu t t_B \eta$ the counting rate due to photons defined above, p_d the probability of a dark count, and $p_s=1-f$ here. The amount of errors in the sifted key is called the quantum bit error rate (QBER, Q). Moreover, this key is not secret: Eve knows a fraction I_{Eve} of it. Some classical postprocessing (error correction and privacy amplification) allows us to extract a key that is errorless and secret, while removing a fraction $h(Q)+I_{\mathrm{Eve}}$, where h is binary entropy. Then,

$$R_{\mathrm{sk}}=R_s(\mu)[1-h(Q)-I_{\mathrm{Eve}}]. \tag{4}$$

With this figure of merit, we can compare our scheme to BB84 implemented using the interferometric bases X and Y, as it is done today, with an asymmetric use of the bases such that $p_s=1-f$ ($\mathrm{BB84}_{XY}$). We require that all the visibilities are equal: $V_X=V_Y$ in $\mathrm{BB84}_{XY}$, $V_{1-0}=V_d$ in our scheme—otherwise, Alice and Bob abort the protocol. Under this assumption, the QBER of BB84 is $Q(\mu)=\{R[(1-V)/2]+(1-R)p_d\}p_s/R_s\equiv Q_{\mathrm{opt}}+Q_{\mathrm{det}}$; while in our scheme $Q(\mu)=Q_{\mathrm{det}}$, independent of V.

In order to estimate I_{Eve}, we restrict the class of Eve's attacks,[6] waiting for a full security analysis. Because of losses and the existence of multiphoton pulses, Eve can gain full information on a fraction of the bits without introducing any errors. This fraction is either $r=\mu(1-t)$ or $r=\mu/2t$, according to whether PNS attacks do not or do introduce errors.[2,6] Then Eve performs the intercept-resend attack on a fraction p_{IR} of the remaining pulses. In $\mathrm{BB84}_{XY}$, she introduces the error $(1-r)p_{\mathrm{IR}}\frac{1}{4}=(1-V)/2$ and gains the information $I=(1-r)p_{\mathrm{IR}}\frac{1}{2}=1-V$. On the present protocol, the IR will be performed in the time basis, so $I=(1-r)p_{\mathrm{IR}}$. However, since we use only one decoy sequence, if Eve detects a photon in two successive pulses she knows what sequence to prepare; the introduced error is then $1-V=I\xi$ with $\xi=2e^{-\mu t}/(1+e^{-\mu t})$ the probability that Eve detects something in one pulse and nothing in the other. Plugging $Q(\mu)$ and $I_{\mathrm{Eve}}=r+I$ into Eq. (4), we have R_{sk} as an explicit function of μ; Alice and Bob must choose μ in order to maximize it. The result of numerical optimization is shown in Fig. 2.[10] As expected, the present protocol is more robust than $\mathrm{BB84}_{XY}$ against the decrease of visibility.

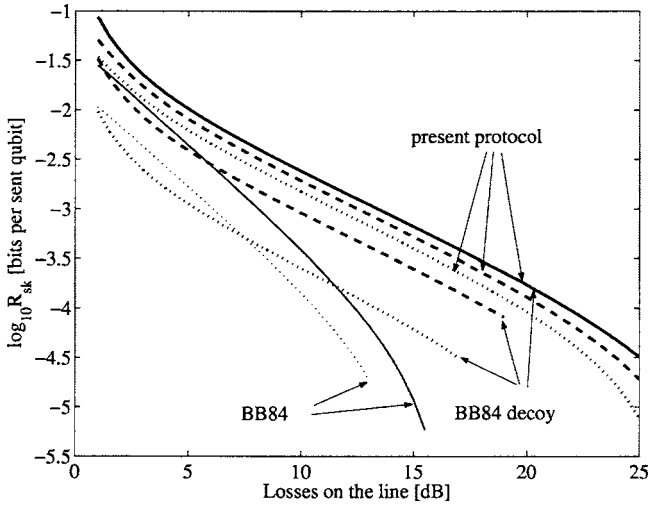


FIG. 2. An estimate of the secret key rates, Eq. (4), for the present protocol and for $\mathrm{BB84}_{XY}$ with and without decoy states, as a function of the losses on the line l ($t=10^{-l/10}$). Parameters: $\eta=10\%$, $p_d=10^{-5}$, $t_B=1$, and $f=0.1$. Visibility: $V=1$ (full lines, identical for the two first protocols), $V=0.9$ (dashed lines), and $V=0.8$ (dotted lines; $R_{\mathrm{sk}}=0$ for BB84 without decoy states).

We show that a reasonably low QBER and good visibility can be obtained using standard telecom components in an implementation with optical fibers. The experimental setup is sketched in Fig. 3. The light of a cw laser (wavelength 1550 nm) passes through an intensity modulator (IM), which prepares the chosen pulse sequence. For simplicity, we send always the same eight-pulse sequence as shown in the figure, namely the string $D010$, where D stands for a decoy sequence. The frequency of 434 MHz of clock C_1 defines the time τ between two successive pulses. The frequency of logical bits in a sequence is half this frequency. The clock C_2 at

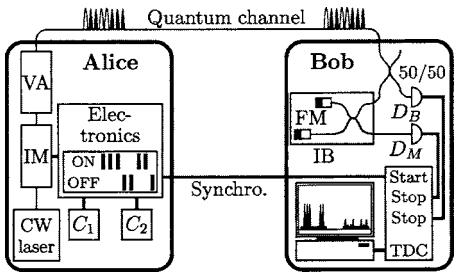


FIG. 3. Experimental setup.

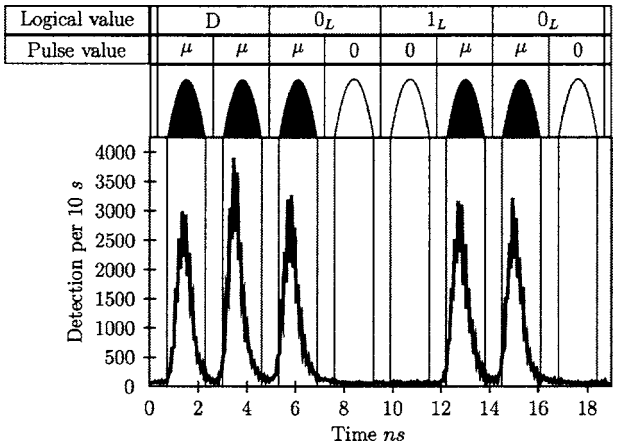


FIG. 4. Detection as a function of the difference of time between start and detection. Logical values and pulse values are depicted in more of the measurement. The difference of amplitude of the different peaks is due to the variation in efficiency in the detection gate.

600 kHz generates the delay between two successive sequences. After the modulator, the light is attenuated by the variable attenuator (VA) in order to obtain $\mu=0.5$ for 5 dB loss in the quantum channel.[10] The synchronization signal directly starts the time-to-digital converter (TDC) and triggers the detectors on Bob's side. The detectors D_B (dataline) and D_M (monitoring line) are opened with gates of 25 ns accepting the whole sequence, featuring quantum efficiency $\eta=10\%$ and a dark count probability $p_d=2.5\times10^{-5}$ per ns. Of course, due to the dead time of the detectors, only one event per sequence and detector can be detected. The stop signal from D_M arm is delayed, which allows us to record the events of both detectors by the same TDC. The Michelson interferometer of the monitoring line has the same pathlength difference τ (46 cm of optical fiber) corresponding to the clock frequency. It is enclosed in an insulated, temperature controlled box (IB). The phase can be changed by changing the temperature. The interferometer (hence our entire setup) is polarization insensitive due to Faraday mirrors (FM) and features a classical fringe visibility of 99%.

The raw detection rate is of 17.0 ± 0.1 kHz. The detection rate is limited by the detectors, due to the 10 μs dead time we have to introduce in order to limit afterpulses. With current detectors, the potential of an improved setup continuously sending pulses at the frequency of C_1, with optimized values for μ, f, and t_B, could only be exploited at long distances. Otherwise, one could use a detection system based on up-conversion and fast thin silicon detector.[11]

The QBER for the pulse sequences "10" and "01" is obtained by considering the time windows of 1.7 ns, as indicated in Fig. 4. The value is $Q=5.2\pm0.4\%$. The contribution of the detector noise and afterpulses (which are rather high for the long gates and high repetition rates we are using) is estimated to be 4%; we attribute the remaining 1% to unperfect intensity modulation, mainly due to too slow electronics and to the jitter of the detectors.

The visibility of the interfering pulses on detector D_M is measured by varying the phase (i.e., the temperature) of the interferometer. The raw visibility is $V_{\mathrm{raw}}\geqslant92\%$, if we consider 1.7 ns time windows. The net visibility, obtained deducing the dark counts and afterpulses, is $V\approx98\%$. We attribute the slight reduction of the visibility to a nonperfect overlap of the interfering pulses due to timing jitter and fluctuations in the intensity modulation. However, this reduced visibility has no significant consequence on the secret key rate (Fig. 2). This tolerance in visibility simplifies the adjustment of the interferometers. With our basic thermal stabilization the interferometer needed to be readjusted only about every 30 min. Indeed, for our pathlength difference, a temperature stability of 0.01 K guarantees $V\gtrsim80\%$. Note that, as the clock frequency of C_1 increases, the stabilization of the interferometer becomes easier.

We have introduced a scheme for QKD and presented the experimental results. The scheme features several advantages: The dataline is very simple, with low losses at Bob's side and small optical QBER. The scheme is tolerant against reduced interference visibility and is robust against PNS attacks (thus allowing the mean photon number to be large, typically $\mu\approx0.5$). Finally, it is polarization insensitive. The existence of such a scheme shows that the main limiting parameter for practical quantum cryptography are the imperfections of the detectors.

The authors acknowledge financial support from the Swiss NCCR "Quantum photonics" and the European Project SECOQC, and thank Avanex for the loan of an intensity modulator.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[3] C. H. Bennett and G. Brassard, in *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[4] Our dataline is that of a classical communication channel, but with a photon counter. The same line is used in a different QKD protocol: T. Debuisschert and W. Boucher, Phys. Rev. A **70**, 042306 (2004).
[5] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005); see also quant-ph/9803007.
[6] N. Gisin *et al.*, quant-ph/0411022.
[7] A similar argument applies to a different protocol: K. Inoue and T. Honjo, Phys. Rev. A **71**, 042305 (2005).
[8] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[9] Alternatively, the source could be a pulsed mode-locked laser followed by a pulse picker.
[10] If dark counts can be neglected ($Q_{\mathrm{det}}=0$), the optimization can be done analytically: for the present protocol, $\mu_{\mathrm{opt}}\simeq V/[2(2-V-t)]$; for BB84, $\mu_{\mathrm{opt}}=f(V)/[2(1-t)]$ with, and $\mu_{\mathrm{opt}}=tf(V)$ without decoy states, where $f(V)=\{V-h[(1-V)/2]\}$. For simplicity, in the optimization we have taken $t_B\approx1$ for both protocols, although this may be technically harder to achieve in BB84 because there are more optical components.
[11] R. Thew *et al.* (in preparation).

Journal of Modern Optics
Vol. 52, No. 18, 15 December 2005, 2637–2648

Taylor & Francis
Taylor & Francis Group

A Fabry–Perot-like two-photon interferometer for high-dimensional time-bin entanglement

DAMIEN STUCKI*, HUGO ZBINDEN and NICOLAS GISIN
Group of Applied Physics, University of Geneva,
20 rue de l'École-de-Médecine, CH-1211 Geneva 4, Switzerland

(*Received 25 February 2005*)

We generate high-dimensional time-bin entanglement using a mode-locked laser and analyse it with a two-photon Fabry–Perot interferometer. The dimension of the entangled state is limited only by the phase coherence between subsequent pulses and is practically infinite. In our experiment a picosecond mode-locked laser at 532 nm pumps a non-linear potassium niobate crystal to produce photon pairs by spontaneous parametric down-conversion (SPDC) at 810 and 1550 nm.

1. Introduction

Entanglement is one of the most useful resources for quantum information [1]. Most entanglement based experiments involved two-level or eventually three-level systems [2–4]. However over the last few years systems with higher dimensions have received increasing attention for a variety of reasons. The tolerance to noise of quantum key distribution can be increased thanks to high-dimensional systems [5]. High-dimensional entanglement allows for the required efficiency of detectors to close the detection loophole in Einstein, Podolsky, Rosen (EPR) experiments to be reduced [6]. Moreover, some properties like the violation of local realism are stronger with high-dimensional systems than with two-level systems and they have greater robustness against noise [7, 8].

High-dimensional systems can be obtained in two ways. Firstly, we can get multi-photon (more than 2) entanglement by using high-order parametric down-conversion [9–11]. Secondly, we can consider two-photon entanglement in high-dimensional systems. This second approach has the experimental advantage of higher coincidence count rates as you have to create and detect only two photons. For example entanglement of higher order angular momentum states of photons has been demonstrated [12, 13]. However, time-bins seem to be the ideal scheme for higher dimensional entanglement. Indeed, a mode-locked laser can easily produce

*Corresponding author. Email: Damien.Stucki@physics.unige.ch

Journal of Modern Optics
ISSN 0950–0340 print/ISSN 1362–3044 online © 2005 Taylor & Francis
http://www.tandf.co.uk/journals
DOI: 10.1080/09500340500283821

entangled states of almost arbitrarily high dimensions. This has been shown using Michelson interferometers [14, 15], i.e. two-dimensional analysers. Unfortunately, the extension of this analysis to higher dimensions, using e.g. interferometers with n different paths, dramatically complicates the experimental task. In this paper, we present an experimental realization of a high-dimensional analysis using Fabry–Perot-like interferometers. We start with a theoretical description of our analyser before presenting the experiment and the results.

2. Theory

A mode-locked laser is used to pump a non-linear crystal in order to produce time-bin entangled photon pairs. We consider a D-pulse train and assume a pair creation probability much lower than $1/D$ per pulse to reduce the creation of two pairs in a D-pulse train. When a photon pair is created in time-bin j, the state is $|j,j\rangle$. As the time-bin in which the photon pair is created is uncertain, the state after the non-linear crystal is of the form:

$$|\psi_{\text{crystal}}\rangle = \sum_{j=1}^{D} c_j e^{i\phi_j} |j,j\rangle \tag{1}$$

where c_j are the probability amplitudes and ϕ_j are the phase differences between successive pulses. For a mode-locked pump laser c_j and ϕ_j are constant.

To analyse the high-dimensional time-bin entangled state we use Fabry–Perot-like interferometers (see figure 1). During one turn through the interferometer a photon is delayed exactly by one time-bin $\Delta\tau = 1/f_{\text{laser}}$ where f_{laser} is the repetition frequency of the laser. Let us first consider the detectors D_a and D_b. After the interferometers where the two photons go to detectors D_a and D_b, respectively, the state $|j,j\rangle$ evolves as follows (the first passage through the interferometer to

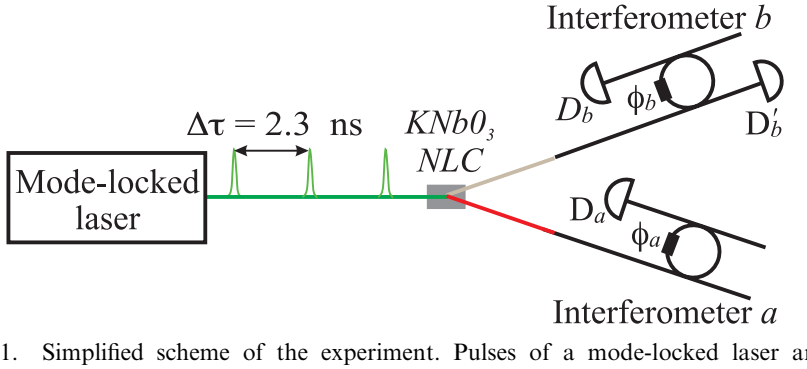


Figure 1. Simplified scheme of the experiment. Pulses of a mode-locked laser are sent through a $KNbO_3$ non-linear crystal (NLC) to produce photon pairs. The two output modes are coupled into separated fibres and go through interferometers with optical paths corresponding to the distance between two successive pulses.

the detectors adds only a global phase, which is not taken into account):

$$
\begin{aligned}
&\vdots \\
&\quad + e^{i\phi_a}|j+1,j\rangle + e^{i(2\phi_a+\phi_b)}|j+2,j+1\rangle + e^{i(3\phi_a+2\phi_b)}|j+3,j+2\rangle + \cdots \\
|j,j\rangle \rightarrow &\quad + |j,j\rangle + e^{i(\phi_a+\phi_b)}|j+1,j+1\rangle + e^{i2(\phi_a+\phi_b)}|j+2,j+2\rangle + \cdots \\
&\quad + e^{i\phi_b}|j,j+1\rangle + e^{i(\phi_a+2\phi_b)}|j+1,j+2\rangle + e^{i(2\phi_a+3\phi_b)}|j+2,j+3\rangle + \cdots \\
&\vdots
\end{aligned}
\tag{2}
$$

where ϕ_x is the phase applied on the photons in mode $x = a, b$ and can be considered constant for successive turns.

The first row represents the situation when photon a covers one more turn than photon b, the second row represents photons a and b in the same time-bin and the third row represents the case with photon b covering one more turn than photon a.

The state of equation (1) then evolves, according to (2), to:

$$
\begin{aligned}
|\psi\rangle = &\sum_{n=0}^{D-1}\sum_{j=1}^{D-n} c_{n,D}(e^{in\phi_a} + e^{i((n+1)\phi_a+\phi_b)} + \cdots + e^{i(D\phi_a+(D-n)\phi_b)})|j+n,j\rangle \\
&+ \sum_{m=1}^{D-1}\sum_{j=1}^{D-m} \tilde{c}_{m,D}(e^{im\phi_b} + e^{i(\phi_a+(m+1)\phi_b)} + \cdots + e^{i((D-m)\phi_a+D\phi_b)})|j,j+m\rangle.
\end{aligned}
\tag{3}
$$

To analyse the system we measure the difference in the time of arrival of photons a and b at detectors D_a and D_b, respectively. For each value of n or m from equation (3) there is a corresponding peak in the histogram of the time difference $\Delta t = t_b - t_a$. The central and highest peak corresponds to coincidences with $\Delta t = 0$, while the first peak on its right corresponds to $\Delta t = \Delta\tau$ and first peak on its left to $\Delta t = -\Delta\tau$ (see figure 2).

The relative height of these peaks, i.e. the probability of coincidences between D_a and D_b for different Δt, can be calculated as follows (for $D \rightarrow \infty$ and without losses):

$$
\begin{aligned}
P_{n=0} \equiv P_0 &\sim (t_{1a}t_{1b}t_{2a}t_{2b})^2 \left|\frac{1}{1 - r_{2a}r_{2b}r_{1a}r_{1b}e^{i(\phi_a+\phi_b)}}\right|^2 \\
P_{n<0} &= (r_{2a}r_{1a})^{2|n|}P_0 \\
P_{n>0} &= (r_{2b}r_{1b})^{2n}P_0
\end{aligned}
\tag{4}
$$

where:

- P_n is the coincidence probability between D_a and D_b for the n-th peak in the arrival time difference histogram. By convention we denote the peak corresponding to photons doing the same number of turns in each interferometer by $n = 0$, the first peak to the right is denoted by $n = 1$, and so on and similarly with peaks on the left $n = -1$ for the first one, and so on.

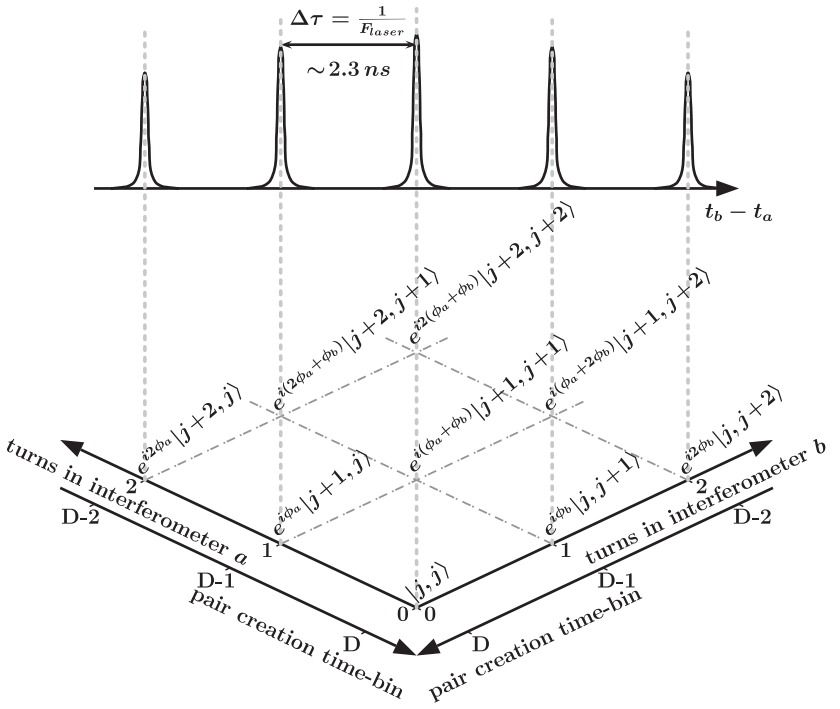


Figure 2. Coincidences as a function of the difference in arrival time for the two photons at detectors D_a and D_b. These correspond to the sum of different interfering terms which are due to the different possibilities for each possible arrival time difference.

- t_{mx} and r_{mx} are the transmission and amplitude respectively of the first ($m=1$) or second ($m=2$) coupler in the interferometer $x=a,b$. By convention a 'reflected' photon stays in the same fibre. One has to choose $t_{mx} \ll r_{mx}$ in order to have strong weighting of the terms that involve many turns in the interferometers, which are characteristic of high-dimensional entanglement.

For all P_n terms the phase dependence is the same for all n so the different peaks of coincidences in the gate of detection on D_b show synchronous oscillations as a function of the sum of the phases in the interferometers, $\phi_a + \phi_b$.

It is interesting to also calculate the probability of having coincidences between the detectors D_a and the third detector D'_b that we use as a control (see figure 1):

$$
\begin{aligned}
P'_{n=0} &\equiv P'_0 \sim \left(\frac{t_{1a}t_{2a}}{r_{1b}}\right)^2 \left| -r_{1b}^2 + \frac{t_{1b}^2 r_{2a} r_{2b} r_{1a} r_{1b} e^{i(\phi_a+\phi_b)}}{1 - r_{2a} r_{2b} r_{1a} r_{1b} e^{i(\phi_a+\phi_b)}} \right|^2 \\
P'_{n<0} &= (r_{2a} r_{1a})^{2(|n|-1)} P'_0 \\
P'_{n=1} &\equiv P'_1 \sim (t_{1a} t_{2a} t_{1b}^2 r_{2b})^2 \left| \frac{1}{1 - r_{2a} r_{2b} r_{1a} r_{1b} e^{i(\phi_a+\phi_b)}} \right|^2 \\
P'_{n>0} &= (r_{2b} r_{1b})^{2(n-1)} P'_1
\end{aligned}
\tag{5}
$$

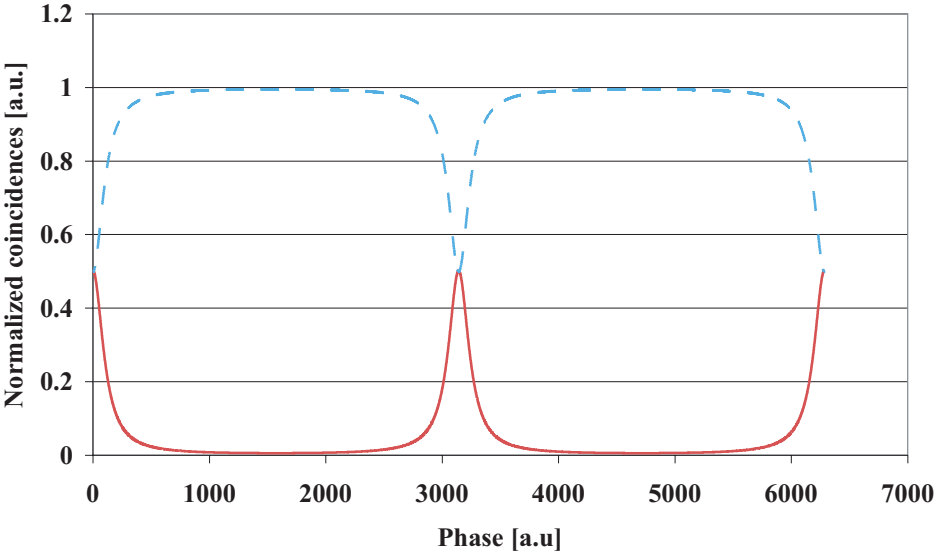


Figure 3. Simulation of normalized coincidences as a function of the phase. The solid line corresponds to coincidences between D_a and D_b and the dashed line corresponds to coincidences between D_a and D'_b ($D \to \infty$, $r_{mx} = \sqrt{0.9}$).

where:

- P'_n is the coincidence probability between D_a and D'_b for the n-th peak in the histogram of arrival time difference. As for P_n we use the convention that $n = 0$ for the case when photons in modes a and b go to the detectors with the same number of complete turns, $n = -1$ for the first peak on its left and so on and $n = 1$ for the first peak on its right, and so on. Note that this histogram is asymmetrical, as all peaks for $n > 0$ are much smaller than those for $n \leq 0$, since $t_{1b} \ll r_{1b}$.

The P' terms show the same behaviour as the P terms, however we have a minimum of coincidences with detector D'_b when we have a maximum of coincidences with detector D_b as can be expected by conservation of energy. Indeed, the light has to go out of the interferometer b by one of the two outputs if there is no losses (absorption) in the interferometers. This different behaviour for the two terms is due to the minus sign in front of r_{1b}^2 in the formula of P'_0 which is a consequence of the $\pi/2$ phase acquired when a photon is 'transmitted', i.e. coupled. In figure 3 we can easily verify that these probabilities sum up to unity in the case without losses. We see that as a function of $\phi_a + \phi_b$, we do not obtain a sinusoidal variation as we are used to in the case of qubits. The curves remind us of the transmission through a Fabry–Perot interferometer, which is a consequence of the high dimensionality of interferences, i.e. many interfering paths. The goal is now to find this signature experimentally.

3. Experiment

A mode-locked, frequency-doubled Nd-laser (Time-Bandwidth GE-100, $\lambda = 532$ nm, FWHM < 10 ps, $F_{\text{laser}} = 430$ MHz, $P_{\text{mean}} = 30$ mW) is the heart of our experiment (see figure 4). A $f_1 = 200$ mm achromatic doublet lens focalizes the light on a potassium niobate non-linear crystal ($KNbO_3$, Castech, $\theta = 23°$, $\varphi = 0°$) cut in order to obtain collinear signal and idler at 810 nm and 1550 nm wavelengths by type I parametric down-conversion. A dichroic mirror is used to separate the two non-degenerate photons. In each output arm, a lens is firstly used to collimate the beam while the second one focuses light into the monomode optical fibre at 810 nm and 1550 nm, respectively. As usual we also have to be very careful to filter out all photons originating from the pump. First we remove the remaining photons at 1064 nm, using a KG5 filter, a dispersive equilateral prism and a diaphragm. In order to remove the pump photons at 532 nm after the crystal, we put a RG-610 filter

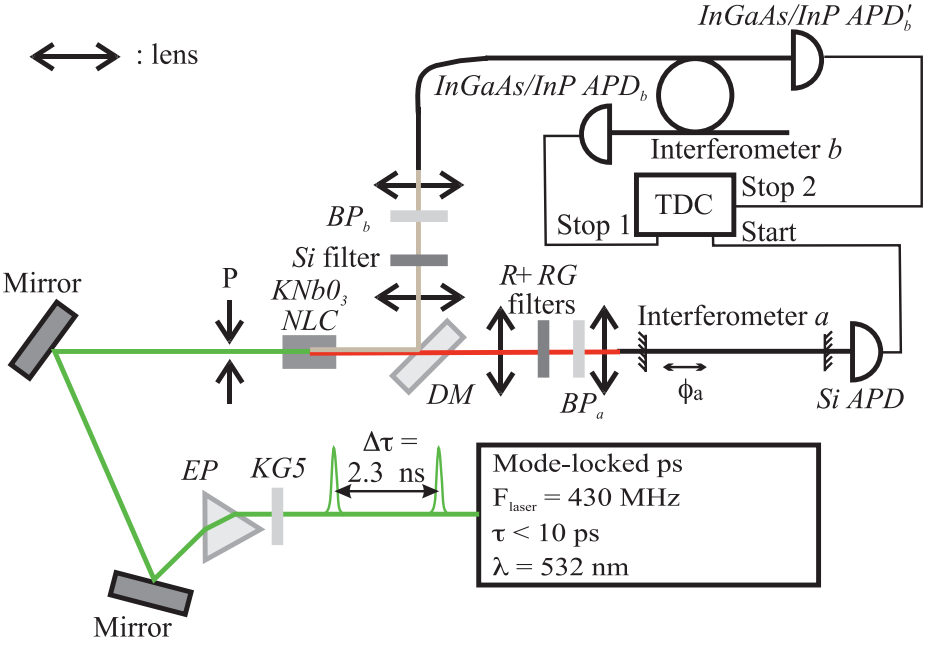


Figure 4. Experimental scheme. The pulses of the mode-locked laser are sent through a KG5 filter, an equilateral prism (EP) and a pinhole (P) to be monochromatic. After that they go through a $KNbO_3$ non-linear crystal (NLC) and produce non-degenerate photon pairs at 810 and 1550 nm by type I parametric down-conversion. The photons at 810 nm are transmitted through a dichroic mirror (DM) and the photons at 1550 nm are reflected. The photons in the 810 nm arm are filtered by a reflector at 532 nm deposited on a RG-610 filter (R + RG filters) and a bandpass filter of 10 nm (FWHM) centred at 810 nm (BP_a). The photons in the 1550 nm arm are filtered by a Si and a bandpass filters of 20 nm (FWHM) centred at 1550 nm (BP_b). The photons are coupled into monomode (at their wavelengths) fibres and go through the interferometers. Detection on the Si APD D_a triggers (not represented) the InGaAs/InP APD's (D_b and D'_b) and starts the TDC. Detections on the InGaAs/InP detectors stop the TDC.

coated with a dielectric mirror at 532 nm and a 10 nm (FWHM) bandpass filter at 810 nm in arm *a* and a combination of an AR coated silicon filter and a 20 nm (FWHM) bandpass filter at 1550 nm in arm *b*.

The interferometer *b* is made of two $R/T = 90/10$ couplers which are spliced together to the required length. An in-line fibre polarization controller (Newport PolaRite F-POL-IL) is added in this loop. The realization of interferometer *a* is different to simplify alignment with the interferometer *b* (see figure 4). It is made from a monomode fibre at 810 nm of about 23.6 cm length with dielectric mirrors deposited on the cleaved extremities with reflectivity and transmitivity $R/T = 90/10$. The fibre is cut slightly shorter than it normally should be and then it is stretched with a translation stage. A piezoelectric actuator (PZT) allows us to then vary the length, i.e the phase, by a few wavelengths. Both interferometers are enclosed in separated PI (proportional and integral parameters) temperature-regulated boxes.

Alignment of the interferometers is the first experimental problem. The optical path lengths of interferometers *a* and *b* must be the same to within the coherence length of the photon pairs, i.e 120 μm, as well as the cavity length of the pump laser, to within the coherence length of the pump (~2 mm in fibre). We use an auxiliary, bulk Michelson interferometer where the path length difference is firstly adjusted to interferometer *b*, using low coherence interferometry. We then adjust the cavity length of the laser and of the interferometer *a* to the auxiliary Michelson interferometer.

The 810 nm photons are detected by a silicon (Si) single photon detector in passive mode (EG&G PQ-F830) and the 1550 nm photons are detected by a InGaAs/InP single photon detector (ID Quantique, id 200 SPDM) gated by the Si detector. The gate width is 50 ns so we can detect 20 time-bins in each gate. The Si detector output starts the Time-To-Digital Converter (TDC, ACAM AM-F1) and one stop is given by each output of the two InGaAs/InP detectors D_b and D'_b.

4. Results

Figures 5(a) and (b) show typical histograms for the time difference between a click from detector $D_a - D_b$ and $D_a - D'_b$, respectively, recorded with the TDC. In case (a) the number of accumulated coincidences is much lower than in case (b), because most of the light is reflected on the first coupler of interferometer *b* and goes directly to the detector D'_b. The vertical lines represent the different time windows used in the measurements of figure 6. In all measurements we record the number of coincidences as a function of ϕ_a, which is a function of the PZT voltage. For this purpose, we accumulate the number of coincidences, typically for 1 min, then increase, step by step, the voltage on the PZT. In order to minimize fluctuations due to varying pump power or coupling of the down-converted photons into the fibres, we normalize all coincidence rates with respect to the average single count rates of detector D_a. We also subtract the noise of InGaAs/InP detectors, whereas the dark-count of the Si detector (D_a) can be neglected. The noise of the InGaAs/InP detectors is due to the thermal dark count of the detector and it is 15.6 ± 0.1 Hz

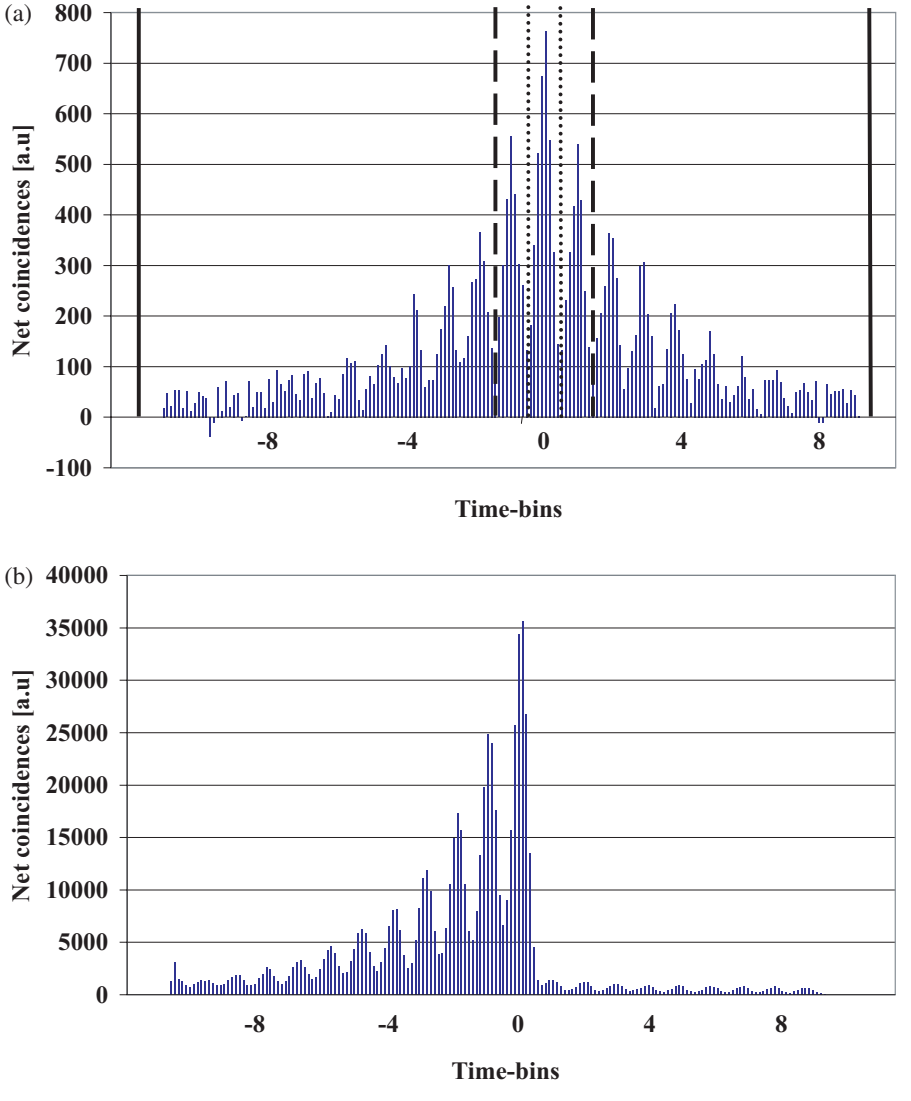


Figure 5. Net coincidences as a function of the difference of arrival times. The histograms are the accumulation of a long term measurement. (a) Histogram between detectors D_a and D_b. The vertical lines represents the different coincidence gates for figure 6, for the complete gate (solid line), the three central peaks (dashed line) and the central peak (dotted line). (b) Histogram between detectors D_a and D'_b. In the case (a) the accumulated coincidences is lower than in case (b) because $T \ll R$.

on D_b and 17.6 ± 0.1 Hz on D'_b for an efficiency of detection of about 16 and 18%, respectively, for the entire gates of 50 ns and a gating frequency of about 4.6 kHz.

This gating frequency corresponds to the rate of detection on the Si detector and it can be explained as follows. The repetition frequency of the laser is 430 MHz and the incident power on the crystal is approximately 17 mW and we have a probability

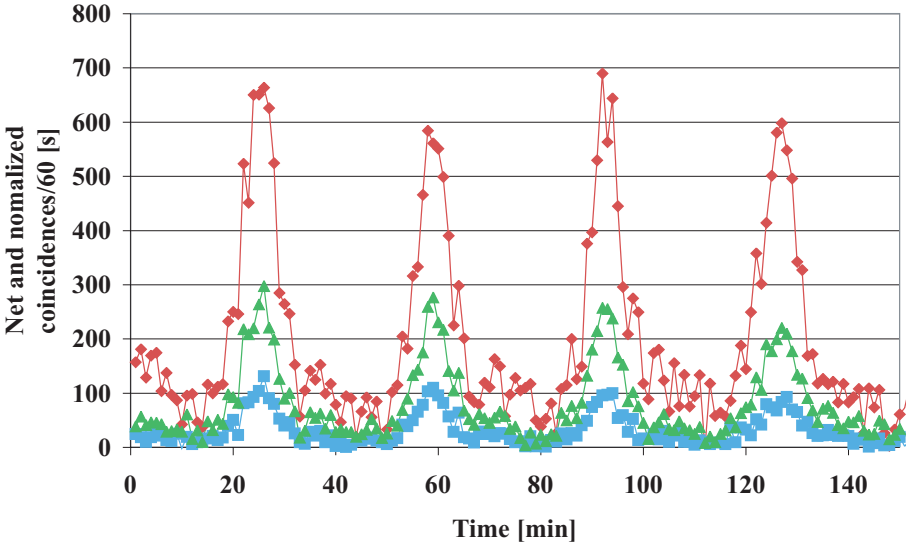


Figure 6. Net and normalized coincidences between Si detector D_a and InGaAs/InP detector D_b as a function of time while changing the phase (see text). We see interferences for the central peak (■), the three central peaks (▲) and the entire gate (about 20 peaks, ♦) (see figure 5). The lines are only presented as a guide.

of pair creation lower then 1%, thus we have a pair creation frequency of < 4.3 MHz. We can expect a global coupling factor of the order 10% between the crystal and the monomode fibre at 810 nm (including the losses through the filters). Therefore 430 kHz of photons at 810 nm are coupled into the fibre. With the losses of about -14 dB when the light goes through the interferometer a and a detection efficiency for the Si detector of the order of 40–50% we can expect a detection frequency of few kHz.

Firstly, we observe that the coincidences between D_a and D_b vary synchronously for all different detection windows. In figure 6 we see the coincidences accumulated over the entire gate of 50 ns, the three central peaks and only the central peak, respectively. These three different coincidences sets oscillate synchronously as expected.

We notice that the peaks are considerably broader than what we would expect for the ideal case according to equation (4) and depicted in figure 3. Of course the experiment is not perfect and we can improve our theoretical model in order to take into account the following four experimental limitations:

(a) There are losses in the order of 5% per round-trip for interferometers a and b. The losses essentially reduce the contribution for the cases where both photons make several round-trips in the interferometers.
(b) High visibility interferences can only be achieved if the polarization states of the interfering paths are identical. For this purpose, we inject in the interferometer, light from an external and pulsed laser, polarized in the same

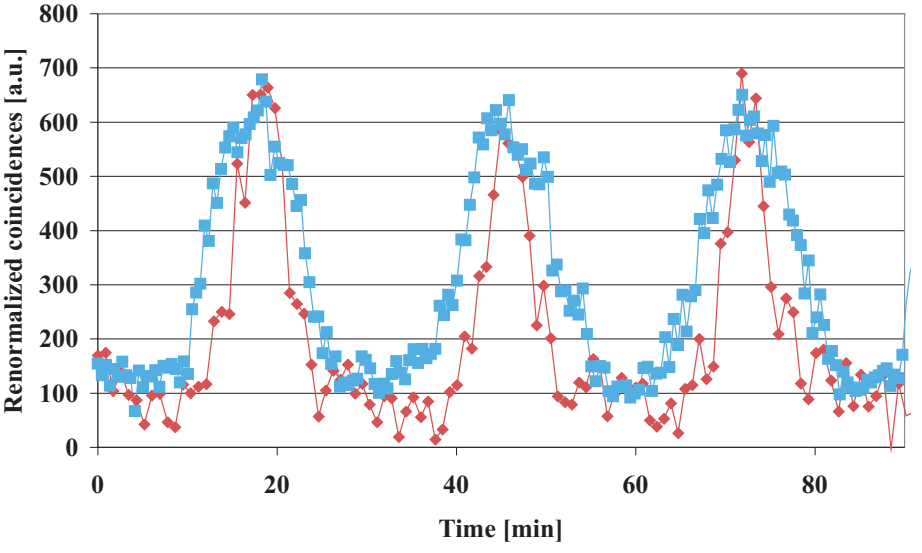


Figure 7. Coincidences as a function of time (see text) with two different fixation systems for the fibre in interferometer *a* for the entire 50 ns InGaAs/InP detector gate. In the first case the fibre is squeezed within a metallic holder (■) and in the second case the fibre is glued on a metallic holder (♦). The first measure is renormalized to have the same amplitude and time dependance.

direction as the down-converted photons. We introduce then an auxiliary polarizer at the output of the interferometer. With the internal polarization controller, we now maximize the transmission of all the peaks, corresponding to zero, one, two and more round-trips in the interferometer. Unfortunately, perfect alignment is very difficult to achieve in practice and the remaining misalignment increases with the number of round-trips. In the interferometer *a* we do not have a polarization controller, we count on the fact that in a short straight fibre, without stress induced birefringence, the polarization is not altered, in principle. However, we have to pay attention to stress induced birefringence. In particular we realized that the peaks are narrower if we glue the fibre on a holder rather than fixing it by squeezing it in metallic holders (see figure 7).

(c) We have to take into account that our light is not monochromatic and hence the phase is not exactly the same for all wavelengths.

(d) Moreover, a slight fluctuation in temperature during the measurement can introduce some phase noise in the order of $\pi/8$ per 0.01°C. Again, this phase noise adds up with each round-trip and is hence more important for the terms characterizing the high-order entanglement.

We try to take into account these experimental limitations. We consider the losses as mentioned above and also the effective spectrums. The most limiting bandpass filter is the 20 nm at 1550 nm one and it corresponds to a bandpass filter of 5.4 nm at 810 nm. Finally we introduce Gaussian phase fluctuations

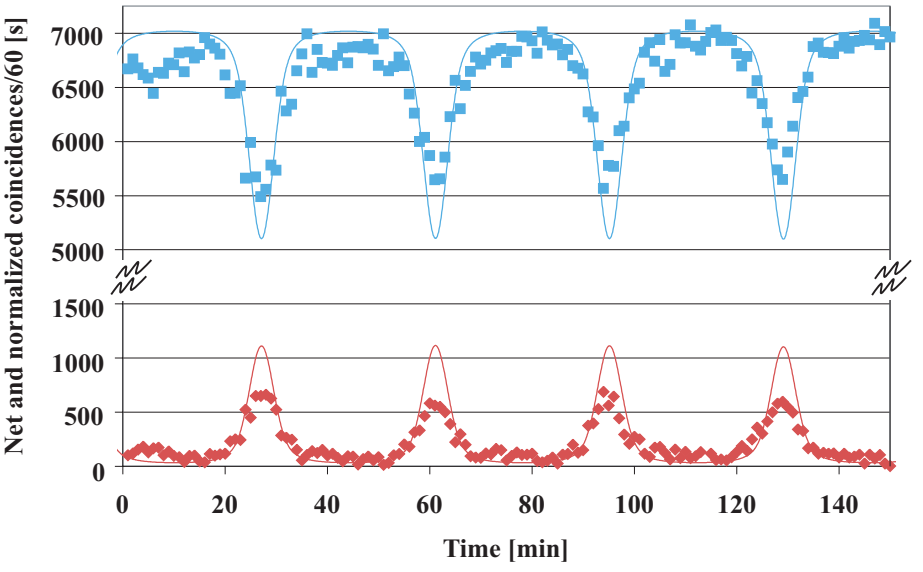


Figure 8. Measurements and simulations of coincidences as a function of time (see text) for the entire 50 ns InGaAs/InP detector gate. The measured coincidences between detector $D_a - D_b$ ($D_a - D'_b$) are represented by ♦ (■). For the simulations we consider the spectra of 5.4 nm at 810 nm and 20 nm at 1550 nm and Gaussian fluctuations on the phase of about $\pi/8$ FWHM corresponding to a length fluctuations of ±25 nm of interferometer *a*.

of $\pi/8$ (FWHM). We can qualitatively reproduce the measured curves (see figure 8). Hence, we conclude that we have demonstrated the generation and the detection of high order entanglement.

5. Conclusions

We experimentally demonstrated high-order time-bin entanglement. Whereas the creation of high-dimensional states is very convenient with mode-locked lasers, we have to realize that the experimental difficulties for detection increase significantly with the dimension of the Hilbert space. Therefore, despite some potential advantages of high-dimensional entangled states discussed in the introduction, these states tend to be of limited value for near-future practical applications.

Acknowledgments

This project was supported by European IST project RamboQ and the Swiss NCCR quantum photonics. We would like to thank Michel Moret (GAP-B, University of Geneva) for his technical support, Andreas Friedrich (IAP, University of Bern) for his help with dielectric coatings, Sofyan Iblisdir for helpful discussions and Rob T. Thew for the attentive reading of the paper.

References

[1] W. Tittel and G. Weihs, Quantum Inform. Comput. **1** 3 (2001).
[2] R. Thew, A. Acín, H. Zbinden, *et al.*, Phys. Rev. Lett. **93** 010503 (2004).
[3] G. Molina-Terriza, A. Vaziri, J. Řeháčcek, *et al.*, Phys. Rev. Lett. **92** 167903 (2004).
[4] N.K. Langford, R.B. Dalton, M.D. Harvey, *et al.*, Phys. Rev. Lett. **93** 053601 (2004).
[5] N.J. Cerf, M. Bourennane, A. Karlsson, *et al.*, Phys. Rev. Lett. **88** 127902 (2002).
[6] S. Massar, Phys. Rev. A **65** 032121 (2002).
[7] D. Kaszlikowski, P. Gnacinski, M. Żukowski, *et al.*, Phys. Rev. Lett. **85** 4418 (2000).
[8] D. Collins, N. Gisin, N. Linden, *et al.*, Phys. Rev. Lett. **88** 040404 (2002).
[9] A. Lamas-Linares, J.C. Howell and D.Bouwmeester, Nature **412** 887 (2001).
[10] J.C. Howell, A. Lamas-Linares and D. Bouwmeester, Phys. Rev. Lett. **88** 030401 (2002).
[11] H. Weinfurter and M. Żukowski, Phys. Rev. A **64** 010102 (2001).
[12] A. Mair, A. Vaziri, G. Weihs, *et al.*, Nature **412** 313 (2001).
[13] A. Vaziri, G. Weihs and A. Zeilinger, J. Opt. B: Quantum Semiclass. Opt. **4** S47 (2002).
[14] H. de Riedmatten, I. Marcikic, H. Zbinden, *et al.*, Quantum Inf. Comput. **2** 425 (2002).
[15] H. de Riedmatten, I. Marcikic, V. Scarani, *et al.*, Phys. Rev. A **69** 050304 (2004).