UNIVERSITÉ DE SHERBROOKE
Faculté de génie
Département de génie électrique et de génie informatique

DISTRIBUTION QUANTIQUE DE CLÉS AVEC DES PHOTOMULTIPLICATEURS DIGITAUX À BASE DE SILICIUM

Mémoire de maitrise
Spécialité : génie électrique

Simon CARRIER

Sherbrooke (Québec) Canada

Septembre 2023

MEMBRES DU JURY

Jean-François PRATTE

Directeur

Serge CHARLEBOIS

Codirecteur

Frédéric MAILHOT

Évaluateur

Marc-André TÉTRAULT

Évaluateur

RÉSUMÉ

Les ordinateurs quantiques sont une technologie prometteuse qui pourrait permettre de faire des calculs qui sont impossibles pour les ordinateurs modernes dans un temps raisonnable. D'autre part, les techniques cryptographiques modernes se basent sur des problèmes computationnels difficiles pour assurer leur sécurité. Ainsi, l'arrivée des ordinateurs quantiques pourrait sévèrement compromettre la sécurité des techniques courantes. La distribution quantique de clés (QKD en anglais) est une façon de distribuer des clés de cryptage secrètes qui utilise des propriétés quantiques. Ceci fait en sorte qu'un malfaiteur (même avec un ordinateur quantique) ne pourrait pas essayer d'intercepter le message sans courir la chance d'induire des erreurs dans le message. En QKD, l'information (les qubits) est transmise via des fibres optiques ou l'air libre, mais la distance et la vitesse de transmission est limitée en ce moment. Le but de ce projet est de faire un circuit intégré qui servirait de détecteur pour un receveur QKD. Il utilisera des PDC (Photon-to-Digital Converter) et l'électronique rapide de 65 nm TSMC afin de livrer un receveur à haut débit. L'avantage d'un PDC est qu'il offre la possibilité d'adapter le détecteur pour l'application. Dans ce cas, du traitement de données et un circuit de fenêtrage ont été ajoutés pour rendre le receveur plus efficace. Le PDC contient aussi des TDC (time-to-digital converter) qui mesurent le temps d'arrivée des photons détectés. Parmi mes contributions originales, j'ai développé, implémenté et validé un circuit de fenêtrage pour les TDC ainsi qu'un circuit de catégorisation pour le QKD. Dans ce mémoire et dans l'article publié (chapitre 7), je présente ces contributions et je démontre ainsi que les PDC peuvent être des receveurs QKD qui offrent une excellente performance temporelle (22.7 ps gigue temporelle) qui est très attrayante pour le QKD. Le but du projet était de démontrer l'avantage des PDC et la tâche a été accomplie. Toutefois, il y a certains éléments qui pourraient améliorer les performances du système. Par exemple, les senseurs monophotonique utilisés étaient des SPAD (Single Photon Avalanche Diode) temporaires afin d'avoir un signal réaliste pour l'électronique. Dans les itérations futures, et avec l'avancement d'autres projets au sein du groupe de recherche GRAMS, des SPAD optimisés pourraient être utilisés afin d'améliorer la sensibilité à la lumière et réduire de bruit d'obscurité du système. De plus, des efforts devraient être mis sur l'uniformisation des performances des composantes au travers de la matrice de pixel du PDC. Des travaux sur des meilleurs formes de calibration des pixels sont en cours.

Mots-clés : Détecteur monophotonique, Distribution quantique de clés, CMOS, QEYSSat, BB84, Internet quantique, Sécurité des données, Time-to-digital converter, Single-photon avalanche diode

À ma famille

REMERCIEMENTS

J'aimerais remercier mes directeurs Jean-François Pratte et Serge Charlebois ainsi que l'équipe du GRAMS pour leur support et patience. J'aimerais aussi remercier ma famille pour leur encouragement et support moral.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LEXIQUE

Terme technique	**Définition**
Time-bin	Type d'encodage pour les qubit (temps et phase)
Superposition	Quand le système est considéré être en plusieurs états simultanément
Decoy State	État utilisé pour détecter Eve
Alice	L'intiateur d'échange de clés (gentil)
Bob	La destination du message d'Alice (gentil)
Eve	Malfaiteur voulant intercepter le message (agresseur)

LISTE DES SYMBOLES

Symbole	**Définition**
$\langle \vert \rangle$	Notation bra-ket
$\vert \rangle$	Un état du système
$\vert \Psi \rangle$	Fonction d'onde d'un système quantique
ϕ	Phase
V ou $\uparrow$	Polarisation Verticale
H ou $\rightarrow$	Polarisation Horizontale
D ou $\nearrow$	Polarisation Diagonale
A ou $\nwarrow$	Polarisation Antidiagonale

LISTE DES ACRONYMES

Acronyme	**Définition**
QKD	Quantum Key Distribution (Distribution Quantique de clés)
CI	Circuit Intégré
IC	Integrated Circuit
GRAMS	Groupe de Recherche en Appareillage Médical
PCB	Printed Circuit Board
BB84	Bennett-Brassard 1984
SiPM	Silicon Photomultiplier
3DdSiPM	3D digital Silicon Photomultiplier (terme remplacé par PDC)
SPAD	Single Photon Avalanche Diode
FPGA	Field-Programmable Gate Array
PMT	Photomultipler Tube
TDC	Time-to-Digital Converter
MZI	Mach-Zehnder Interferometer
RSA	Rivest-Shamir-Adleman (algorithme d'encryption asymétrique)
ECC	Elliptic-Curve Cryptography
AES	Advanced Encryption Standard
DES	Data Encryption Standard
3DES	DES appliqué 3 fois
DS	Decoy State
PNS	Photon Number Splitting (Attack)
DCA	Detector Control Attack
PDC	Photon-to-Digital Converter

CHAPITRE 1

INTRODUCTION

La sécurité informatique est un élément essentiel de tous les jours. Que ce soit un appel téléphonique ou une transaction bancaire, la sécurité et la confidentialité de l'information transmise sont très importantes. Par contre, le système parfaitement sécuritaire n'existe pas. Il y aura toujours des failles dans un système. Le but est de les mitiger le plus possible afin de minimiser le risque. Par exemple, la cryptographie couramment utilisée dans les systèmes de télécommunication moderne (ex.: RSA) se base sur des calculs mathématiques complexes et coûteux pour permettre des transmissions sécurisées. Un malfaiteur pourrait prendre une clé publique RSA et calculer la clé privée associée, mais cela lui prendra tellement de temps (souvent dans l'ordre des milliers d'années) qu'il ne sera pas possible d'avoir la clé à temps pour décrypter les données. Par contre, avec l'avènement des ordinateurs quantiques, cela pourrait changer. Des ordinateurs quantiques pourraient, en théorie, faire les calculs cryptographiques nécessaires pour compromettre les systèmes courants dans un temps raisonnable. C'est pour cette raison que la cryptographie quantique a pris beaucoup d'ampleur ces dernières décennies: la technologie quantique arrive finalement à mettre en pratique les théories et le besoin d'assurer la sécurité de l'information de demain devient de plus en plus pressant. Malgré que la télécommunication quantique a encore beaucoup de chemin à faire avant de devenir monnaie courante, la distribution quantique de clés est une technologie réalisable aujourd'hui avec un impact significatif.

La distribution quantique de clés (Quantum Key Distribution, QKD) est une technique cryptographique de transfert de mots de passe secrets entre deux groupes via un canal quantique. En d'autres mots, on distribue des clés de cryptage/décryptage avec l'aide de technologies quantiques. Expliquons d'abord la différence entre un canal quantique et un canal classique. Dans le cas du canal classique, l'information transmise est sous forme binaire (1 ou 0), mais dans le cas quantique, ce sont des qubits. Les qubits peuvent représenter un 1, un 0 ou une superposition des deux (on dit ici, une combinaison). Un qubit peut avoir plusieurs implémentations physiques: le spin d'un électron ou la polarisation d'un photon par exemple. C'est cette dernière qui est souvent utilisée en communication quantique. Une des particularités importantes des qubits: quand on décide de les observer (c.-à-d. mesurer) pour voir dans quels états ils sont, ils tombent à un état fixe (au lieu d'une superposition de 0 et 1). Ainsi, l'ordre des observations a un impact. En autres mots,

le simple fait d'observer un état quantique (le qubit ici) influence les résultats des observations subséquentes. Cette dernière caractéristique est très importante. Dans le cadre de la transmission d'informations quantiques, ceci veut dire que si un malfaiteur (nommée Ève) veut écouter la conversation entre deux parties (nommés Alice et Bob), Ève a une forte chance de changer le message en cours de route. Un autre aspect très important de la physique quantique est le théorème de non-clonage. Ce théorème dit qu'il est impossible de dupliquer un état quantique inconnu. Donc, si Alice et Bob communiquent avec des qubits, Ève ne peut pas lire le message en cours de route sans la possibilité de le changer et ne peut pas faire une copie du message sans le lire. Ce sont ces raisons pour lesquelles la communication quantique est si attrayante: la physique quantique garantit qu'il est impossible d'intercepter un message en transit sans l'influencer [56].

Évidemment, l'histoire n'est pas aussi simple. Il y a beaucoup de défis à relever afin de faire une communication quantique robuste. En effet, la création de qubits, le maintien de leur état quantique durant leur transmission et leur lecture à la destination sont des tâches non triviales. La distribution quantique de clés est donc un compromis intéressant. On distribue les clés secrètes de Alice à Bob avec l'aide du canal quantique, mais on fait la transmission de messages cryptés avec ces clés sur le canal classique (internet, radio, etc.). Le but est d'éventuellement avoir un réseau global de QKD afin d'échanger des clés sur de longues distances. Une façon prometteuse est de faire ceci par des satellites [31]. Mais, pour ce faire, il faut des receveurs QKD avec hauts débits (bitrate), peu de pertes, peu de bruit et intégrables dans des espaces limités en volume et poids. C'est un véritable défi interdisciplinaire (physique quantique, ingénierie, optique, électronique) qu'il faudra résoudre avant l'arrivée des ordinateurs quantiques.

L'objectif de ce projet est la conception, l'implémentation et la validation d'un détecteur monophotonique en CMOS 65 nm servant à recevoir des échanges QKD. Ce prototype vise à démontrer l'avantage qu'un circuit intégré avec traitement de signaux embarqués offre pour des applications quantiques comme le QKD.

Pour accomplir ceci, 3 éléments novateurs ont été développés pour cette puce. Le premier était TDC gating: une technique pour éliminer les évènements hors de notre fenêtre temporelle d'intérêt. Le second est du traitement de signal dans la puce spécialisée pour le QKD. Finalement, le troisième est l'ajout d'une matrice 8×8 de SPADs (Single Photon Avalanche Diode) pour avoir une plus grande surface photosensible. Nous avons utilisé pour cette première version de la puce les SPAD développés dans cette technologie qui ne sont pas optimisés pour la tâche: ils ont plus de bruit thermique et moins de sensibilité que voulu, mais ils fournissent des signaux réalistes pour le restant du système. Cependant,

pour tester la chaine de traitement complète, du circuit de lecture du SPAD à l'information numérique obtenue par traitement dans la puce, ces SPADs seront suffisants. Ce document commence par une mise en contexte de la théorie, suivi des avancées les plus récentes dans le domaine. Ensuite, la problématique sera expliquée plus en détail. Finalement, la section développement explorera la conception, les méthodes et caractérisations, les résultats et la discussion.

CHAPITRE 2

ÉTAT DE L'ART

Malgré que la distribution quantique de clés (QKD) soit un domaine assez nouveau (1984), il y a beaucoup d'aspects à explorer afin de comprendre les motivations à exploiter le QKD, comment les milieux de recherches et industiels implémentent le QKD en ce moment, quelle sont les problèmes connus et dans quelle direction se dirige la communauté ? Cette section va explorer ces questions en commençant par un historique rapide de la physique quantique. Ensuite, il sera question de BB84: le premier protocole de cryptographie quantique et son fonctionnement. Ceci sera suivi par une exploration des composantes des systèmes courants et les alternatives à la polarisation. Finalement, un résumé des performances des systèmes courants sera exploré.

2.1 Historique rapide de la physique quantique

Il faut un peu de contexte historique de la physique quantique pour comprendre la distribution quantique de clés. La mécanique quantique date du temps des travaux de Max Planck sur la radiation de corps noir en 1900 [48]. C'est depuis Planck que les physiciens ont découvert de plus en plus de phénomènes que la physique classique ne pouvait pas totalement expliquer. Vers les années 1920, des physiciens comme Schrödinger, Born et Heisenberg proposaient ce qui allait être la physique quantique. Ce n'était pas encore clair, mais ils réalisèrent que certains phénomènes s'expliquent bien avec des outils statistiques: les fonctions d'ondes. La mécanique quantique proposait l'idée qu'une particule pouvait avoir plusieurs valeurs de propriété (spin, position, etc.) simultanément et qu'en l'observant elle "décidait" un état.

Le fait que la physique ne soit pas déterministe était en conflit total avec la mécanique classique. Notamment, en 1935, le fameux papier d'Einstein-Podolsky-Rosen [19] est publié. Ils argumentent que la physique quantique est une théorie incomplète et qu'il doit exister des "variables cachées". Selon eux, la physique quantique ne ferait que les approximer avec des éléments statistiques et si ces variables cachées étaient découvertes, alors une vraie théorie ferait surface. Ce n'est qu'en 1964 que John Bell publie un papier [3] qui démontre avec appuis mathématiques que, peu importe la quantité de "variables cachées", il serait impossible de reproduire les prédictions validées expérimentalement par la physique quantique. Ce résultat est crucial: la nature à très petite échelle n'est pas régie par des lois

déterministes ! Armées avec ce nouvel outil mathématique qu'est la physique quantique, beaucoup d'expériences se sont développées afin de mieux comprendre des phénomènes connus et développer de nouvelles applications qui utilisent ces phénomènes. Des transistors aux fibres optiques, bien des technologies n'auraient pas été poussées sans la physique quantique. Le grand défi scientifique de nos jours est l'ordinateur quantique. L'ordinateur quantique est une idée qui a gagné beaucoup d'attention après la proposition de Richard Feynman en 1982 [21]. En effet, il suggérait que de telles machines seraient capables de faire des simulations et calculs que les ordinateurs classiques sont incapables de faire dans un temps raisonnable. L'idée derrière est simple: pour simuler un monde quantique, il faut un ordinateur quantique. Par contre, il s'avère que les ordinateurs quantiques sont aussi difficiles à faire qu'ils sont intéressants. Encore à ce jour, malgré qu'il existe des pseudo-ordinateurs quantiques, il n'existe aucun vrai ordinateur quantique tolérant aux erreurs. La question alors devient: si les ordinateurs quantiques n'existent pas encore, pourquoi est-ce que la communauté pousse autant la recherche en QKD ? La raison pour ceci est que, selon la théorie, les ordinateurs briseraient complètement le cryptage de l'internet moderne. La section suivante va plus en détails.

2.2 La menace inévitable

Il existe 2 grands types de cryptographies: symétrique et asymétrique. Ils servent différentes fonctions essentielles à l'internet d'aujourd'hui.

- Cryptographie symétrique.
  - Cryptage avec clés symétriques. (DES (obsolète), 3DES, AES)
  - Chiffrement par flux (ou-exclusif entre le message à chriffer et une clé aussi longue que le message)
  - Fonctions de hachage (ex: MD5, SHA-1,2,3)
  - Génération de nombres aléatoires
- Cryptographie asymétrique.
  - Cryptage par clés publiques (asymétrique) (RSA, ECC)
  - Signatures numériques

La cryptographie symétrique est une approche où les deux groupes partagent la même clé. Le plus simple et efficace est le "Masque jetable" ("One-time Pad" en anglais) où une clé secrète connue par les deux parties est utilisée pour crypter le message une seule fois et ensuite une autre clé est utilisée. Or, distribuer une clé secrète n'est pas chose facile et souvent des algorithmes intelligents comme AES sont utilisés afin de pouvoir utiliser la clé secrète plus d'une fois. Il y a aussi les fonctions de hachage: ce sont des fonctions unidirectionnelles qui convertissent un message de longueur aléatoire à un message de

longueur fixe. Ces fonctions agissent comme des boites noires et sont souvent utilisées pour valider l'intégrité d'un message. Par exemple, le hachage d'un logiciel est partagé sur les sites web de façon à ce que si on effectue la fonction de hachage sur le logiciel une fois téléchargé et qu'il correspond aux hachages donnés sur les sites web, alors le logiciel n'a pas été modifié malicieusement. Bref, la force de la cryptographie symétrique est qu'elle est rapide, mais n'offre pas de façon facile de distribuer ses clés facilement entre les utilisateurs.

La cryptographie asymétrique est une autre bête. Introduite par Diffie et Hellman en 1976 [18], elle permet qu'il y ait deux clés complémentaires: une clé décrypte ce que l'autre a crypté et vice-versa. Typiquement, une est nommée la clé publique et est partagée avec le monde. L'autre est nommée la clé privée et est gardée secrète par l'utilisateur. Donc, si quelqu'un veut envoyer un message à l'utilisateur, il prend la clé publique de son destinataire et crypte le message avec celle-ci. Seul le détenteur de la clé privée pourra décrypter le message. L'inverse est vrai aussi: si l'utilisateur veut prouver qu'un message vient bel et bien de lui, alors il peut crypter le message avec sa clé privée et n'importe qui avec sa clé publique pourra valider l'authenticité du message. Ces clés sont dérivées de différents problèmes mathématiques dont les solutions sont jugées faciles à vérifier, mais très difficiles à trouver. Par exemple, l'algorithme asymétrique standard d'aujourd'hui, soit RSA, utilise la factorisation de nombre entier. Par exemple, il est facile de démontrer que le produit des deux nombres premiers 151 et 239 est égal à 36089, mais il n'est pas aussi facile de trouver les facteurs premiers de 36089. La force de la cryptographie asymétrique est qu'elle facilite le processus de distribution de clés, mais elle est exigeante en matière de calculs.

Il est facile de voir que ces deux types de cryptographies vont main dans la main. En effet, c'est commun d'utiliser RSA pour s'échanger une clé AES et ensuite poursuivre l'échange de message avec AES, qui est plus efficace. Par contre, chacun de ces types de cryptographie repose sur des hypothèses: ils présument que défaire leur cryptage ne peut pas se faire dans un temps raisonnable. En d'autres mots, si un malfaiteur voulait décrypter un cryptage RSA, cela lui prendrait tellement de temps que l'information lui serait inutile une fois qu'il aura réussi. La seule exception à cette règle est le "Masque jetable", car la clé n'est seulement utilisée qu'une fois. En bref, la cryptographie classique ne se soucie pas d'avoir une sécurité inconditionnelle, elle s'assure que l'information reste sécurisée pour au moins sa durée de vie utile.

Par contre, les ordinateurs quantiques viennent changer les règles du jeu. En 1994, Peter Shor présente un algorithme quantique [58][59] efficace pour la factorisation de nombres

entiers. Un problème qui prend un temps sous-exponentiel pour un ordinateur classique devient polynomial avec cet algorithme. En d'autres mots, il faut beaucoup moins de temps trouver les facteurs premiers d'un nombre entier aléatoire. Ceci est très important, car, comme dit précédemment, cette algorithme brise des méthodes de cryptages asymétriques comme RSA qui dépendent sur la factorisation de nombres entiers très grands.

Deux ans plus tard, en 1996, Grover publie un autre algorithme quantique [27] qui est capable de déterminer l'entrée d'une fonction boite noire avec seulement $\sqrt{N}$ itérations. Donc, une clé de 256 bits (2^{256}) aurait seulement la sécurité d'une clé de 128 bits ($\sqrt{2^{256}} = 2^{128}$). Parce que les ordinateurs quantiques courants ne sont pas assez puissants, ces deux algorithmes ont seulement des démonstrations sur papier. Toutefois, ils représentent des menaces importantes à la cryptographie moderne et des applications tangibles pour les ordinateurs quantiques. Le tableau 2.1 représente l'étendue de l'impact. Il y aura certai-

Algorithme	Niveau de sécurité Pré-quantique	Niveau de sécurité Post-quantique	Algorithme d'attaque
Encryption symétrique			
AES-128	128	64	Grover
AES-256	256	128	Grover
Encryption asymétrique			
RSA-3072	128/256	Brisé	Shor
DSA-3072	128	Brisé	Shor
ECDSA	128/256	Brisé	Shor
ECC	224/256	Brisé	Shor
Fonction de hachage			
SHA-256	256	128	Grover
SHA-3	256	128	Grover

TABLEAU 2.1 Impact des algorithmes quantiques sur les algorithmes populaires aujourd'hui [16].

nement des ordinateurs quantiques, la question est de savoir quand. Malgré qu'il y ait plusieurs estimés [40], le délai avant l'arrivée de l'ordinateur quantique est encore sujet à débat. Par contre, en 2015, la NSA (National Security Agency) aurait annoncé à la communauté de ne pas trop s'investir dans la transition RSA->ECC et plutôt se préparer pour des algorithmes post-quantiques [45] [16] (qui sont classiques, mais plus résistants aux attaques quantiques). Malgré que les motivations derrière cette annonce soient un sujet de beaucoup de discussions [34], elles semblent démontrer l'importance de considérer aujourd'hui les capacités des ordinateurs du futur et la necessité de développer les receveurs QKD aujourd'hui.

2.3 BB84, premier du nom

La distribution quantique de clés (ou QKD) a vu ses débuts en 1984 avec la publication de Bennett et Brassard [7] sur le protocole BB84. Il est le premier protocole de cryptographie quantique, soit un protocole pour faire un échange de clés sécuritaire en utilisant la physique quantique. Ils ont démontré le protocole sur un montage expérimental en 1989 [4] en utilisant comme qubit la polarisation des photons uniques. C'est un montage simple à réaliser en laboratoire sur de courtes distances. Par contre, à longue distance, le problème devient beaucoup plus difficile. Il y a deux éléments essentiels au montage: une source laser monophotonique et un détecteur monophotonique. Souvent, pour des raisons de coûts, le laser monophotonique est un laser très atténué et le senseur monophotonique était un PMT (Photomultiplier Tube). Pour simplifier le montage, des fibres optiques servaient en tant que médium de transmission des photons [38]. Les fibres optiques étaient une façon simple de contrôler le parcours des photons en ayant un certain niveau de contrôle sur le bruit ambiant. Par contre, les fibres optiques ont des lacunes: elles permettent difficilement de conserver la polarisation des photons, elles sont affectées par la température et, après une certaine distance, le signal devient trop atténué [2]. Pour ce dernier point, normalement, on pourrait mettre un répéteur sur la fibre optique pour augmenter le signal de nouveau, mais il est impossible de faire ceci avec des photons dans des états quantiques. En effet, dû au théorème de non-clonage, il n'est pas possible de dupliquer un état quantique inconnu. Il faudrait observer le photon avant de le retransmettre, ce qui briserait le principe même de la distribution quantique de clés. Bref, des répéteurs quantiques ne sont pas encore disponibles. Pour contourner les limitations des fibres optiques, certains ont exploré le QKD dans l'air libre [14]. Les années passèrent et de nouveaux protocoles ont été proposés. Certains comme B92 [6] ou SARG04 [55] sont des évolutions de BB84. D'autres proposèrent d'utiliser des protocoles avec des photons intriqués comme E91 [20]. Par contre, BB84 reste tout de même le protocole plus populaire. Il est simple et reste le seul protocole à avoir une preuve mathématique de sa sécurité cryptographique [60].

2.4 Alice, Bob et Ève entrent dans un bar...

Cette section décrit un échange de clés secrètes avec le protocole BB84. Il est utile de connaître les acteurs typiquement utilisés dans le domaine: Alice, Bob et Ève. Alice est la personne qui initie un échange sécurisé avec son ami Bob[1]. L'objectif est qu'Alice puisse

1. La raison pour le nom Alice est simplement, car le nom commence avec A. Même raison pour Bob.

échanger un message avec Bob (B). Ève[2] est l'intruse qui veut intercepter le message sans que Alice et Bob ne le remarquent.

Comme dit précédemment, BB84 utilise la polarisation pour transmettre l'information. Plus spécifiquement, il utilise deux bases non orthogonales: horizontale/verticale (H/V ou +) et diagonale/anti-diagonale (D/A ou ×). Chaque base a un 1 et un 0. Posons arbitrairement: horizontale est 1, vertical est 0, diagonale est 0 et anti-diagonale est 1. La raison pour laquelle les deux bases doivent être non orthogonales sera évidente sous peu. Par contre, avant de commencer l'échange de messages, deux éléments cruciaux sont nécessaires. Alice et Bob doivent avoir un canal quantique (pour la transmission des qubits) et un canal classique *authentifié*. Ce dernier est absolument nécessaire pour que Alice sache qu'elle parle bel et bien à Bob et vice-versa. Sans ce canal classique authentifié, Ève pourrait voler l'identité de Bob ou Alice et intercepter les messages (Man-in-the-Middle Attack). La procédure d'échange de clés se déroule comme suit. L'interférence de Ève sera considérée plus tard.

1. Alice choisit une polarisation qu'elle veut envoyer. Elle pourrait envoyer V ou D pour envoyer un 0 ou H ou A pour un 1. Le tableau 2.2 résume ceci.

Base	Valeur 0	Valeur 1
+	↑	→
×	↗	↘

TABLEAU 2.2 Bases et états du qubit avec l'encodage par polarisation

2. Alice polarise un seul photon conformément à ce choix et elle l'envoie à Bob

3. Parce que Bob ne connaît pas dans quelle base Alice a envoyé le qubit (le photon), il doit choisir aléatoirement la base pour faire sa mesure. Si Bob a choisi la même base que Alice (par exemple, H/V), alors la mesure du qubit lui révèlera la bonne polarisation (à savoir H donc un bit de 1 ou V soit un bit de 0). Si Bob choisit la mauvaise base, le résultat de la mesure sera aléatoirement 0 ou 1, sinon il obtiendra la bonne polarisation d'Alice. La raison de ce comportement vient de la nature quantique du qubit et du fait que les bases sont non orthogonales. Par exemple, un photon polarisé H, quand lut au travers de la base D/A a autant de chance d'être mesuré comme un photon polarisé D que A. On dit ainsi que H est une superposition des états D et A. En effet, une superposition se résume à un état $|\Psi\rangle$ qui peut être

2. Nommée après "(Eave)sdropper", anglais pour une personne qui écoute une conversation sans autorisation.

représenté par la combinaison linéaire de deux états simultanément:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

où $\alpha^2 + \beta^2 = 1$
$\alpha, \beta \in \mathbb{C}$

$$|\Psi\rangle_H = \frac{|0\rangle_D + |1\rangle_A}{\sqrt{2}} \tag{2.2}$$

avec $\alpha = \beta$

4. Une fois que Bob a choisi sa base et a lu le qubit de Alice, il garde secrète la valeur du bit obtenue. Il déclare ensuite à Alice sur le canal classique authentifié (important !) quelle **base** il a choisi pour la lecture. Il transmet donc soit l'information H/V ou D/A ce qui ne révèle pas la valeur du bit obtenue. Alice lui indique si cette base est la bonne ou pas. Si le choix de base est bon, Bob garde le résultat de la mesure. Si le choix n'est pas bon, Bob rejette la mesure. On appelle cette étape le «tamisage» (sifting). On peut voir dans le tableau 2.3 un exemple d'échange où tous les scénarios sont représentés.

5. Les étapes 1 à 4 se répètent N fois. Comme Bob se trompe de base 50% du temps, Alice et Bob obtiennent la même clé d'une longueur $\frac{N}{2}$ en moyenne.

Bit d'Alice	0	1	0	1	0	1	0	1
Base d'Alice	+	+	+	+	×	×	×	×
Polarisation du Photon	↑	→	↑	→	↗	↘	↗	↘
Base choisie de Bob	+	+	×	×	+	+	×	×
Résultat lu par Bob	↑	→	↗ *ou* ↘	↗ *ou* ↘	↑ *ou* →	↑ *ou* →	↗	↘
Clé conservée	0	1	jeté	jeté	jeté	jeté	0	1

TABLEAU 2.3 Table de vérité des échanges possibles entre Alice et Bob

L'étape 3 exige un peu d'explication. Bob a 50% de chances de se tromper de bases. Ceci cause en moyenne une diminution de la clé utile de moitié. C'est un grand prix à payer, mais c'est pour cette raison que l'échange reste sécuritaire. C'est ici que Ève s'ajoute dans le scénario. Pour réitérer: Ève veut lire le message que Alice envoie à Bob, sans qu'ils ne le remarquent. Le scénario où Ève intercepte les qubits de Alice et les retransmet à Bob est une attaque de la forme "Intercept and Resend". Les étapes se déroulent comme suit:

1. Alice prépare et envoie un qubit à Bob sur le canal quantique.

2. Ève intercepte ce message. Ève doit maintenant faire un choix de base pour lire le qubit et, comme Bob, elle a 50% de chances de choisir la mauvaise base. Elle prend le résultat de sa lecture (qui respecte les mêmes règles que dans le tableau 2.3) et le transmet à Bob.
3. Bob reçoit le qubit (de Ève) et applique la même procédure avec 50% chances de choisir la même base que Ève.
4. Bob transmet sur le canal authentifié (mais pas nécessairement sécuritaire, sur lequel Ève peut écouter) sa liste de base. Ève ne peut pas faire pareil, car le canal est authentifié et son message serait automatiquement vu comme le message d'un intrus. Alice confirme ou rejette le choix de base de Bob.
5. Parce que Ève a modifié le qubit envoyé par Alice en faisant sa mesure dans la transmission, les clés résultantes de Alice et Bob ne sont pas identiques. Alice et Bob comparent une partie de leurs clés qui sera jetée par la suite et s'ils remarquent un taux d'erreur élevé dans leurs clés, ils sauront qu'une Ève écoute leur transmission (cette étape est nommée "Réconciliation d'information" et est expliquée plus tard). La transmission est annulée si le taux d'erreur est jugé trop haut.

Base A	Photon d'A	Base E	Résultat d'E	Base B	Résultat de B	Clé conservée
+	↑	+	↑	+	↑	0
	→		→		→	1
	↑	×	↗ *ou* ↘		↑ *ou* →	?
	→					?
×	↗	+	↑ *ou* →			rejeté
	↘					rejeté
	↗	×	↗			rejeté
	↘		↘			rejeté
+	↑	+	↑	×	↗ *ou* ↘	rejeté
	→		→			rejeté
	↑	×	↗ *ou* ↘			rejeté
	→					rejeté
×	↗	+	↑ *ou* →			?
	↘					?
	↗	×	↗		↗	0
	↘		↘		↘	1

TABLEAU 2.4 Échange de qubit avec présence d'Ève sur les canaux

Ce tableau démontre comment la présence de Ève introduit des erreurs dans la transmission. Il y a 16 scénarios et dans 4 de ceux-ci Ève n'induit pas d'erreur additionnelle. Les " ?" indiquent des résultats aléatoires de 0 ou 1 qui contribuent aux erreurs dans la clé qui permettent de détecter la présence d'Ève. Les mesures rejetées sont dues au fait que Bob et Alice ne partagent pas la même base.

Le tableau 2.4 démontre les scénarios possibles avec la présence de Ève. Dans 4 scénarios, Ève n'a pas été détectée et Bob obtient un bit qu'il pense être sécuritaire. Dans 4 autres scénarios (ceux marqués ?), le résultat est aléatoire. Dans ces cas, Ève pourrait être chanceuse et avoir envoyé la même valeur qu'Alice et ils ne remarquent pas la présence d'Ève. Or, si le choix de base de Alice et Bob est vraiment aléatoire, alors 50% du temps, les ? donnerons une mauvaise valeur. En d'autres mots, si Ève intercepte les messages et les renvoie à Bob, elle induit 25% d'erreur en moyenne. Quand Alice et Bob regarderont leurs clés, ils remarqueront ce haut taux d'erreurs. Notez que dans le cas où il n'y a pas d'Ève, l'erreur est théoriquement nulle. C'est un jeu de statistique: plus la clé est longue, plus Ève risque d'induire des erreurs dans la clé.

2.5 Le diable est dans les détails

La section précédente examinait un scénario théorique. En réalité il y a beaucoup d'autres éléments qui entrent en jeu lors de l'échange: le bruit du canal, la performance des détecteurs et la fiabilité de la source de photons sont tous des éléments à tenir compte. Ces problèmes sont encore plus néfastes que dans les systèmes classiques. En effet, comme le QKD cherche à garantir avec un très haut niveau de certitude la sécurité de ses clés, les erreurs additionnelles d'un système imparfait sont associées à une attaque potentielle de Ève. En effet, il est impossible de distinguer une erreur de bruit d'une erreur induite par Ève. Par exemple, s'il y a du bruit sur le canal qui cause que Bob reçoit un 1 au lieu d'un 0. Quand Alice et Bob réalisent cette erreur, ils ne peuvent pas savoir si le bruit venait d'une Ève potentielle ou du canal. Ceci impose des limites très strictes sur les montages QKD. En effet, si les erreurs dans le canal et les systèmes sont trop hautes, il est impossible d'établir des clés sécuritaires. Cette section explore comment la littérature mitige certaines des imperfections des systèmes QKD.

2.5.1 Le bruit dans le canal

Dans ce contexte de QKD, le bruit correspond aux évènements détectés par le receveur qui ne sont pas dus à un qubit. Donc, le bruit est la somme de la lumière ambiante, dans le canal, le bruit thermique du détecteur, etc. Parce que le bruit a tant d'impact sur la viabilité des clés et qu'il est impossible de distinguer des erreurs (les " ?" dans le tableau 2.4) causées par le bruit ou Ève, il faut réduire l'effet du bruit à un minimum. Heureusement, les signaux bruités ne datent pas d'hier et il existe plusieurs solutions au problème. La plus populaire est d'utiliser des codes de correction d'erreur dans les clés. Par exemple, certains bits sont alloués comme bits de parité durant la transmission et Bob peut vérifier si le message contient des erreurs en relations à ces bits de parités. Cette étape est tellement commune qu'elle a un nom: la réconciliation d'information ("Information Reconciliation"

en anglais). Des codes comme LDPC, Turbo ou Polar codes sont d'excellents candidats pour cette étape [56]. Par contre, cette étape a un inconvénient non négligeable. Parce que Alice et Bob s'échangent de l'information sur la validité de leur clé (les bits de parité par exemple) sur le canal classique, Ève peut aussi écouter ces informations. Ainsi, Ève augmente la quantité d'information qu'elle a sur la clé. Ce que Alice et Bob doivent mitiger avec l'étape suivante: "amplification de sécurité".

2.5.2 L'information partielle d'Ève

Tel que vue dans les exemples d'échanges précédents et les tableaux 2.3 et 2.4, peu importe le scénario, Ève peut être chanceuse et obtenir une fraction de la clé sans que Bob et Alice ne s'en aperçoivent. Il est donc dit que Ève peut détenir une information partielle de la clé. De plus, comme dit précédemment, Ève peut aussi gagner de l'information durant la phase de réconciliation d'information. Parce que ceci réduit la force cryptographique de la clé, cela a le potentiel de compromettre le système. Il faut mitiger l'impact de l'information partielle que Ève détient par cette étape nommée phase d'amplification de sécurité (ou "Privacy Amplification" en anglais) [5]. Elle se résume à réduire la longueur de la clé de façon à éliminer avec un certain niveau de certitude l'information que Ève détient. Les fonctions de hachage sont parfaites [56] pour ces applications et ce sont souvent elles qui sont utilisées. Par exemple, Alice et Bob s'avisent qu'ils utiliseront l'algorithme MD5 avec leurs clés corrigées courantes de longueur N. Leurs clés sont maintenant de longueur X où $X < N$ dont la la sécurité augmente avec le nombre de bits sacrifiés $(N - X)$. Parce que Ève n'avait pas la totalité de la clé, elle n'est pas capable de déterminer la valeur de la clé post-hachage.

2.5.3 Imperfection de la source monophotonique

Dans beaucoup de protocoles de QKD, émettre seulement un photon est un critère important. Ceci est dû au fait que si plusieurs photons sont émis, Ève pourrait "voler" une partie des photons et laisser le reste poursuivre leur chemin vers Bob intouchés. Ainsi, Ève gagnerait de l'information sans induire d'erreurs dans les qubits que Bob reçoit. Ce type d'attaque se nomme "Photon Number Splitting Attack" (PNS attack) [12].

Jusqu'à présent, les scénarios explorés avaient toujours une source monophotonique parfaite: la source émet exactement 1 photon au moment voulu. En réalité, ceci est très rarement le cas. En effet, parce que ces sources sont très coûteuses et/ou très restrictives (vitesse de répétition trop basse, longueur d'onde inadéquate, etc.), une source faible cohérente est souvent la solution utilisée. Ces sources sont des lasers normaux avec beaucoup d'atténuation afin de ne conserver qu'un seul photon par impulsion laser. Malheureusement, ces atténuations respectent souvent des distributions de Poisson. Ceci fait en sorte

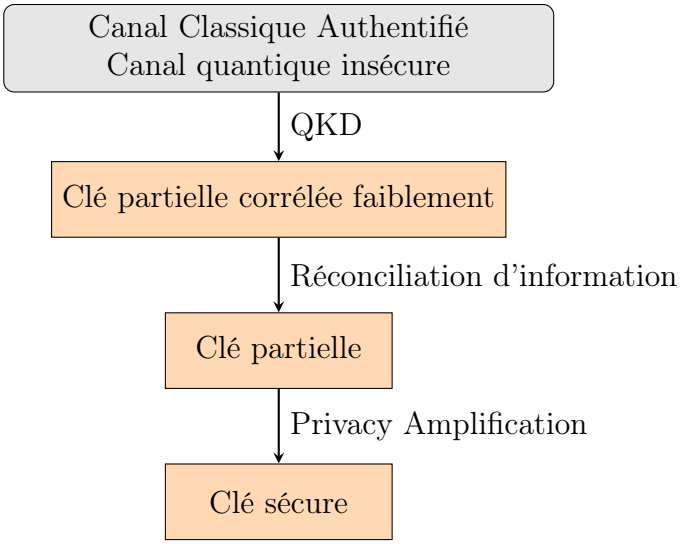

FIGURE 2.1 Séquence des étapes afin d'obtenir une clé sécure.
La partie QKD n'est seulement que la première étape. Comme dit précédemment, afin d'obtenir une clé sécuritaire dont Ève n'a presque pas d'information partielle, il faut passer au travers des étapes de réconciliation d'information et de "Privacy Amplification".

que pour émettre presque jamais plus que 1 photon, la quantité d'émissions avec 0 photon est très haute [25]. Le tableau 2.5 est un exemple de distribution de nombres de photons

Photons par pulse	Probabilité
$\|0\rangle$	0.82
$\|1\rangle$	0.16
$\|2\rangle$	0.016

TABLEAU 2.5 Exemple de distribution de nombre de photons par pulse utilisé pour le QKD.

par émission. Parce qu'avoir 2+ photons est à éviter et avoir juste 1 photon est désiré, la distribution de Poisson cause le cas de aucun photon d'arriver couramment. Évidemment, ceci nuit grandement au taux d'échange de clés. Malgré que la probabilité d'avoir plus de 2 photons soit diminuée, afin d'avoir un système parfaitement sécurisé, il ne faut pas ignorer la possibilité que Ève exploite ces rares moments et gagne de l'information sur la clé. Pour remédier à ce problème, Hwang [30] propose l'idée de "Decoy states" (DS). L'idée derrière ces approches est qu'Alice utilise volontairement plusieurs intensités différentes (une intensité pour les données, et d'autres pour les "decoy") et en faisant des statistiques a posteriori, Alice et Bob peuvent calculer si une attaque PNS est survenue.

2.5.4 Imperfection du détecteur monophotonique

Le canal quantique est souvent fragile et sujet à beaucoup de sources de bruit et d'imperfection. C'est pour ces raisons qu'il faut le meilleur détecteur possible afin de ne pas perdre de précieux qubits qui se sont finalement rendus à destination. Le QKD opère donc dans un régime d'opération dit à "photon unique" ("photon starved"). Ceci implique que le système doit détecter un photon entrant avec une bonne efficacité avec le moins de bruit thermique (ou d'obscurité) possible. De plus, afin d'augmenter le débit de transmission sur la ligne et augmenter la quantité de données par secondes, il faut que le détecteur soit capable de lire les photons à un haut débit (entre 1 MHz et 1 GHz) [28, 44]. Les principales caractéristiques sont résumées dans le tableau 2.6. Il y a donc plusieurs facteurs à prendre

Propriété	Description	Valeur idéale	Facteurs influençant
Sensibilité	La plus petite quantité d'énergie qu'il peut détecter	1 photon	Le matériel photosensible, la technique de détection, etc.
Efficacité de détection	Le rapport de détection sur la quantité réelle d'évènements	100%	Matériel, technique de détection, longueur d'onde
Bruit d'obscurité	Le taux de détection quand il est dans le noir absolu et il ne devrait rien détecter	0	Température d'opération, matériel photosensible, etc.
Temps mort	Le temps nécessaire pour que le détecteur soit prêt pour le prochain évènement.	0	Temps de conversion, temps de relaxation du détecteur, etc.

TABLEAU 2.6 Propriétés principales d'un détecteur photonique [41] [28].

en compte lors du choix de détecteurs et c'est souvent une question de compromis. Par contre, à partir des critères établis précédemment et dans la littérature, il est possible de déterminer les plus importants. Parce que chaque qubit est un photon unique, le premier critère essentiel est une sensibilité monophotonique. Le tableau 2.7 passe en revue les différentes technologies disponibles. Il illustre les points forts et faibles de chacune. Par exemple, les TES (transition-edge sensor) offrent une excellente efficacité de détection dans l'infrarouge et un bruit d'obscurité extrêmement bas, mais ont une gigue temporelle (jitter) très large et un débit de comptage (100 kHz) plus bas que la moyenne (10 MHz).

La spécialisation de notre groupe de recherche se situe dans la catégorie des Si SPAD (shallow junction). La gigue temporelle est parmi les meilleures (35 ps), le bruit d'obscurité est bas (25 Hz), le débit de comptage est dans la moyenne à 10 MHz et sa plage de tempéra-

Table 1 | Comparison of single-photon detectors.

Detector type	Operation temperature (K)	Detection efficiency, η	Jitter time, Δt (FWHM)	Dark count rate, D (ungated)	Figure of merit	Max. count rate	Resolves photon number?	Class of report
PMT (visible–near-infrared)[31]	300	40% @500 nm	300 ps	100 Hz	1.33×10^7	10 MHz	Yes	†
PMT (infrared)[32]	200	2% @1,550 nm	300 ps	200 kHz	3.33×10^2	10 MHz	Yes	†
Si SPAD (thick junction)[38]	250	65% @650 nm	400 ps	25 Hz	6.5×10^7	10 MHz	No	†
Si SPAD (shallow junction)[41]	250	49% @550 nm	35 ps	25 Hz	5.6×10^8	10 MHz	No	†
InGaAs SPAD (gated)[55]	200	10% @1,550 nm	370 ps	91 Hz	2.97×10^5	10 kHz	No	‡
InGaAs SPAD (self-differencing)[57]	240	10% @1,550 nm	55 ps	16 kHz	1.14×10^5	100 MHz	Yes	‡
Frequency up-conversion[65]	300	9% @1,550 nm	400 ps	13 kHz	1.7×10^4	10 MHz	No	‡
Frequency up-conversion[65]	300	2% @1,550 nm	40 ps	20 kHz	2.5×10^4	10 MHz	No	‡
VLPC[69]	6	88% @694 nm	—	20 kHz	—	—	Yes	§
VLPC*	6	34% @633 nm	270 ps	7 kHz	1.83×10^5	—	Yes	§
TES[76]	0.1	50% @1,550 nm	100 ns	3 Hz	1.67×10^6	100 kHz	Yes	‡
TES[20]	0.1	95% @1,550 nm	100 ns	—	—	100 kHz	Yes	§
SNSPD (meander)[90]	3	0.7% @1,550 nm	60 ps	10 Hz	1.16×10^7	100 MHz	No	‡
SNSPD (new)[87]	1.5	57% @1,550 nm	30 ps	—	—	1 GHz	No	§
QD (resonant tunnel diode)[96]	4	12% @550 nm	150 ns	2×10^{-3} Hz	4×10^9	250 kHz	No	§
QD (field-effect transistor)[93]	4	68% @805 nm	—	—	—	1 Hz	Yes	§

The class of report indicates the conditions under which the detector characteristics were measured; † represents a commercial product specification, ‡ represents the use of the detector in a practical experiment and § represents a measurement of device performance. *Unpublished data, Burm Baek, NIST, USA, 2009.

TABLEAU 2.7 Tableau comparatif des différents types de détecteurs monophotoniques [28].

ture d'opération est proche de la température ambiante (250 K). Par contre, sa sensibilité est maximale (50%) approximativement au centre du spectre visible (550 nm). Parce que la majorité des télécommunications se font dans le domaine de l'infrarouge (1550 nm), il n'est pas possible d'opérer dans les infrastructures de télécommunication standard avec ce dispositif. Toutefois, même avec ce désavantage, selon la figure de mérite de Hadfield, cette option est une des meilleures pour le QKD. De plus, les SPAD sont de bons candidats pour une application sur satellite due à leur petite taille et faible demande énergétique [2]. Dans notre groupe, les travaux de Samuel Parent [47] (thèse disponible sur Savoir UdeS) sont concentrés sur le développement de SPAD et de leur intégration 3D avec le partenaire industriel Teledyne DALSA.

Notre groupe détient l'expertise pour la conception du détecteur, mais nous avons besoin d'expert sur l'application de QKD. C'est pour cette raison que ces travaux sont faits

en collaboration avec Thomas Jennewein et Ramy Tannous de l'University of Waterloo (Ontario).

2.6 Approches n'utilisant pas la polarisation

BB84 est un protocole, mais l'utilisation de la polarisation comme encodage n'est pas obligatoire. En effet, BB84 a été initialement proposé avec un encodage par polarisation parce que celle-ci est simple et facile à générer avec de simples filtres polarisants et des séparateurs de faisceau polarisants. Par contre, la polarisation n'est pas sans faille. Changer rapidement de polarisation (et donc différentes bases) n'est pas une tâche facile due à des limites mécaniques du filtre polarisant classique. Or, la plus grande faiblesse est que beaucoup de médiums de transmission, notamment les fibres optiques, souffrent de la dispersion chromatique. Ceci fait en sorte que différentes longueurs d'onde vont se déplacer dans le médium à différentes vitesses. Donc, les pulses vont s'étaler et causer de l'incohérence. De plus, il existe un autre problème dans les fibres optiques: la dispersion des modes de polarisation (Polarization mode dispersion ou PMD) [24]. Ceci est un effet causé par les imperfections biréfringentes dans les fibres et il fait en sorte que différentes polarisations vont se déplacer à différentes vitesses. Ceci a l'effet indésirable que deux qubits adjacents de polarisations différentes pourraient se mélanger et induire des erreurs. Dans l'air libre, la turbulence cause la dépolarisation des photons [29]. Bref, tous ces points font en sorte que la polarisation est un mode d'encodage simple, mais avec bien des problèmes de transmission à surmonter.

Au fil des années, plusieurs autres encodages ont été proposés afin de contourner les points négatifs de la polarisation. Certains proposèrent l'utilisation de modes spatiaux de la lumière pour transmettre des qubits [23], mais le plus intéressant était par l'encodage temporel ("Time-bin") [39]. L'encodage temporel utilise des bases qui sont plus complexes. La première base est le temps d'arrivée du photon qu'on définit comme en avance (early ou $|e\rangle$) ou en retard (late ou $|l\rangle$). La deuxième base est la différence de phase du photon. Plus spécifiquement, c'est la différence de phase (ϕ) entre les états $|e\rangle$ et $|l\rangle$ quand ils sont en superposition. Dans la majorité des cas, ces différences de phase sont destructives ($\phi = \pi$) ou constructives ($\phi = 0$) et les états de cette base sont représentés ainsi:

$$|\Psi\rangle = \frac{|l\rangle + e^{-i\phi}\,|e\rangle}{\sqrt{2}} \tag{2.3}$$

Ainsi, quand $\phi = \{0, \pi\}$ les deux états de la base de phase deviennent:

$$\phi = 0 : \frac{|l\rangle + |e\rangle}{\sqrt{2}} \tag{2.4}$$

$$\phi = \pi : \frac{|l\rangle - |e\rangle}{\sqrt{2}} \tag{2.5}$$

L'encodage temporel et l'encodage par polarisation sont complètement équivalents. Dans les deux cas, il y a deux bases non orthogonales et 2 valeurs possibles dans chaque base. Donc, le tableau 2.2 devient le tableau 2.8 Il est maintenant facile de voir que pour l'en-

Base	Valeur 0	Valeur 1
Temps	$\|e\rangle$	$\|l\rangle$
Phase	$\frac{\|l\rangle+\|e\rangle}{\sqrt{2}}$	$\frac{\|l\rangle-\|e\rangle}{\sqrt{2}}$

TABLEAU 2.8 Bases et états des qubits avec l'encodage temporel

codage temporel, le protocole BB84 peut rester identique, c'est seulement l'encodage, soit comment l'information quantique est encodée dans le qubit, qui change. Voyons maintenant la manière de réaliser cet encodage. Il faut être capable de générer des photons soit en avance $|e\rangle$ ou en retard $|l\rangle$ ou une superposition des deux avec une différence de phase de 0 ($\frac{|l\rangle+|e\rangle}{\sqrt{2}}$) ou de π ($\frac{|l\rangle-|e\rangle}{\sqrt{2}}$). La solution à ce problème est l'interféromètre Mach-Zehnder (MZI) non balancé. La partie non balancée indique seulement qu'un bras de l'interféromètre est plus long que l'autre. La figure 2.2 illustre un système pour créer et lire les qubits avec encodage temporel. C'est une méthode parmi tant d'autres, mais elle est simple et efficace. Le processus peut être fait en 4 étapes:

1. **Généré un photon en polarisation V,H,D ou A.** Cette étape est préparatoire pour ce qui va suivre. Chacune des polarisations sera convertie en un état des bases de l'encodage temporel à la prochaine étape.

2. **Encodage temporel du qubit.** Le photon entre dans un séparateur de faisceau polarisant. Si sa polarisation est H, alors il ira vers le haut dans le bras long du MZI. Si sa polarisation est V, il continuera tout droit dans le bras court. Ces deux possibilités deviennent donc $|l\rangle$ et $|e\rangle$ respectivement. Si sa polarisation est D ou A, alors il passe dans les deux bras simultanément. En effet, contrairement à la physique classique où la réponse aurait été que le photon choisit un chemin aléatoirement, la physique quantique permet le passage du photon par les deux chemins en même

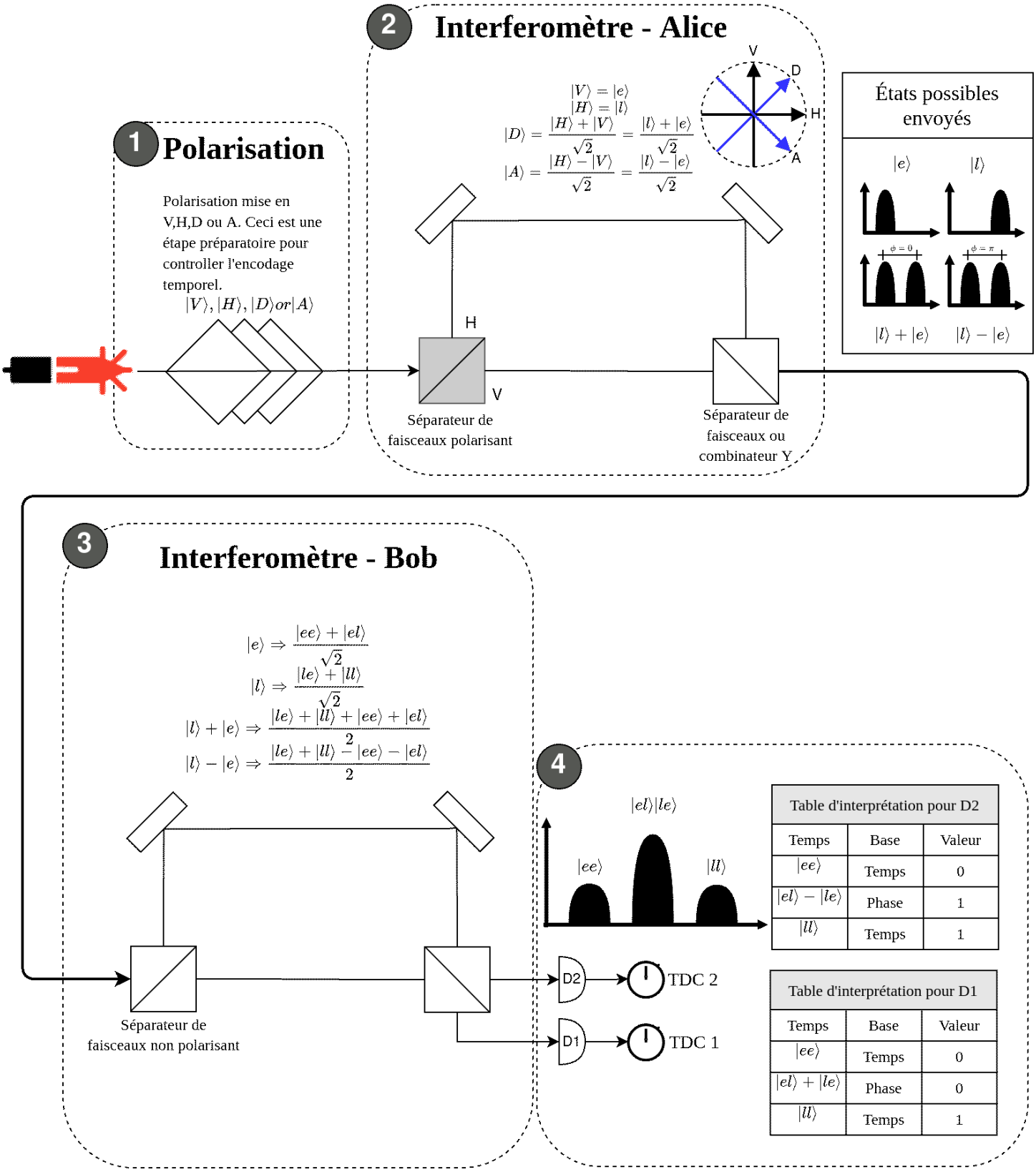

Table d'interprétation pour D2

Temps	Base	Valeur
$\|ee\rangle$	Temps	0
$\|el\rangle - \|le\rangle$	Phase	1
$\|ll\rangle$	Temps	1

Table d'interprétation pour D1

Temps	Base	Valeur
$\|ee\rangle$	Temps	0
$\|el\rangle + \|le\rangle$	Phase	0
$\|ll\rangle$	Temps	1

FIGURE 2.2 Le processus d'échange de clés avec l'encodage temporel. Cette figure illustre seulement comment les qubits sont acheminés et non comment le protocole s'exécute, mais le protocole choisi pourrait être BB84.

temps ce qui mènera à la sortie du MZI à la création d'un état superposé. En effet, D et A peuvent être interprétés comme des superpositions de H et V.

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}}, |A\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}, \tag{2.6}$$

Alors, chacune sera associée à une des superpositions de la base de phase:

$$|D\rangle = \frac{|l\rangle + |e\rangle}{\sqrt{2}}, |A\rangle = \frac{|l\rangle - |e\rangle}{\sqrt{2}}. \tag{2.7}$$

Après le MZI, le photon est transmis sur le canal. Sa polarisation n'est plus importante et peut être dépolarisée par le canal sans problèmes, car l'information quantique est maintenant contenue dans le temps d'arrivée (encodage temporel) du photon. Dans la figure 2.2, les encodages sont représentés par des distributions de probabilités (bosses) des photons sur la base du temps (axe X). Il y a une seule bosse quand le photon est dans un état propre à la base du temps, mais deux bosses quand il est dans une superposition temporelle représentant l'un des deux états propres de la base de phase.

3. **Bob reçoit le photon et le passe dans son propre MZI.** Ce MZI est identique à celui d'Alice à l'exception du premier séparateur de faisceau qui n'est pas polarisant. Il y a 4 situations possibles: une pour chaque valeur possible du qubit entrant. Il est plus facile de démoduler en phase et en temps le photon à l'aide de ce MZI.

$$|e\rangle \overset{MZI}{\mapsto} \frac{|ee\rangle + |el\rangle}{\sqrt{2}} \tag{2.8}$$

$$|l\rangle \overset{MZI}{\mapsto} \frac{|le\rangle + |ll\rangle}{\sqrt{2}} \tag{2.9}$$

$$\frac{|l\rangle + |e\rangle}{\sqrt{2}} \overset{MZI}{\mapsto} \frac{|le\rangle + |ll\rangle + |ee\rangle + |el\rangle}{2} \tag{2.10}$$

$$\frac{|l\rangle - |e\rangle}{\sqrt{2}} \overset{MZI}{\mapsto} \frac{|le\rangle + |ll\rangle - |ee\rangle - |el\rangle}{2} \tag{2.11}$$

L'état $|ee\rangle$ veut dire que le photon a passé par le chemin court dans les deux MZI et l'état $|ll\rangle$ le chemin long dans les deux MZI. $|el\rangle$ le chemin court dans le premier et long dans le deuxième et l'inverse pour $|le\rangle$. Si les deux MZI ont des longueurs de bras identiques, alors $|el\rangle$ et $|le\rangle$ représentent le même décalage temporel. Ils sont donc associés à la même base du milieu et arrivent en même temps au dernier séparateur de faisceau de Bob. Si la différence de signe entre $|el\rangle$ et $|le\rangle$ est +, alors il y a

une interférence constructive ($\phi = 0$) et donc sortira toujours vers le détecteur D1. Toutefois, si la différence de signe entre $|el\rangle$ et $|le\rangle$ est $-$, alors il y a une interférence destructive ($\phi = \pi$) et sortira toujours vers le détecteur D2. Le "choix" de base est aléatoire et hors du contrôle de Bob dans cet arrangement. Le "choix" de quelle base lire est fait passivement par le premier séparateur de faisceau du MZI de Bob.

4. **Bob fait la lecture du qubit aux sorties du MZI.** Il y a 2 sorties possibles au MZI. Une va au détecteur D1 et l'autre au D2. Si le photon est dans un des états temporels satellites ($|ee\rangle$ ou $|ll\rangle$) alors le choix de sortie est aléatoire au séparateur de faisceau et le détecteur doit simplement déterminer le temps d'arrivée (la base temporelle). Comme mentionné à l'étape 3, si le photon est dans le lobe central ($\frac{|le\rangle - |el\rangle}{\sqrt{2}}$ ou $\frac{|le\rangle + |el\rangle}{\sqrt{2}}$), il est impossible de distinguer entre les deux états uniquement par le temps d'arrivée (ils sont tous dans le lobe temporel central). Il faut donc déterminer la différence de phase. Pour ce faire, le photon va interférer avec lui-même à la jonction du dernier séparateur de faisceau. Si la différence de phase cause une interférence constructive ($\phi = 0$) alors le photon sortira par la sortie vers D1. Si, au contraire, l'interférence est destructive ($\phi = \pi$) alors le photon ira vers D2. Ce comportement est une caractéristique des séparateurs de faisceau. Prenons les équations 2.8 à 2.11. Les états en bleu correspondent aux bons choix et en rouge les mauvais choix de bases. Par exemple, dans 2.8 où l'état $|e\rangle$ est envoyé par Alice, $|ee\rangle$ est unique, mais $|el\rangle$ ne peut pas être distingué de $|le\rangle$ (du point de vue du détecteur), car ils sont dans le même lobe temporel. Donc, dans le cas où Bob reçoit $|ee\rangle$, il aura la bonne valeur (0). Mais, s'il reçoit $|el\rangle$, il lit en base de phase. Parce qu'il n'y pas eu d'interférence, le qubit sera détecté par D1 ou D2. Il aura donc 50% de chance d'avoir la mauvaise valeur.

5. **Bob dit à Alice son choix de base.** Même si Bob ne choisit pas activement la base de lecture (temps ou phase), il sait dans quelle base le qubit a été projeté. Par exemple, si le qubit a été détecté dans un des lobes temporels satellites ($|ee\rangle$ ou $|ll\rangle$), il sait que la base choisie était le temps. Si le qubit a été détecté dans le lobe temporel central, la base de phase avait été choisie. À ce point, Bob connaît la base et la valeur, mais ne sait pas si la base utilisée était la bonne. Bob demande donc a Alice si sa base utilisée était correcte. Notez que partager, même publiquement, la base utilisée ne dévoile pas d'information. En effet, partager la base ne donne pas d'information sur la valeur transmisse (0 ou 1). Dans les cas où la bonne base était utilisée, Alice dit à Bob de garder le bit. Dans le cas contraire, Bob rejette le bit complètement.

Le tableau 2.9 correspond à la table de vérité des situations possibles.

Bit d'Alice	0	1	0	1	0	1	0	1
Base d'Alice	T	T	T	T	ϕ	ϕ	ϕ	ϕ
État du photon	$\|e\rangle$	$\|l\rangle$	$\|e\rangle$	$\|l\rangle$	$\frac{\|l\rangle+\|e\rangle}{\sqrt{2}}$	$\frac{\|l\rangle-\|e\rangle}{\sqrt{2}}$	$\frac{\|l\rangle+\|e\rangle}{\sqrt{2}}$	$\frac{\|l\rangle-\|e\rangle}{\sqrt{2}}$
Base de mesure de Bob	T	T	ϕ	ϕ	T	T	ϕ	ϕ
État inféré par Bob	$\|ee\rangle$	$\|ll\rangle$	$\|el\rangle$	$\|le\rangle$	$\|ee\rangle$ *ou* $\|ll\rangle$	$\|ee\rangle$ *ou* $\|ll\rangle$	$\frac{\|le\rangle+\|el\rangle}{\sqrt{2}}$	$\frac{\|le\rangle-\|el\rangle}{\sqrt{2}}$
Clé conservée	0	1	rejeté	rejeté	rejeté	rejeté	0	1

TABLEAU 2.9 Table de vérité des échanges possibles entre Alice et Bob avec encodage temporel.

Le temps(T) et la phase(ϕ) sont les deux bases non orthogonales. Les évènements rejetés sont ceux dont la base de lecture de Bob était mauvaise.

Il y a un point important à propos des MZI dont il faut tenir compte lors de la conception des systèmes. Ceci est le fait que le MZI d'Alice doit être absolument identique à celui de Bob. Ceci est essentiel afin d'assurer que $|e\rangle$ et $|l\rangle$ représentent les mêmes distances parcourues dans les deux systèmes. Si ce n'est pas le cas, les probabilités de distribution ne pourront pas interférer parce que $|el\rangle$ et $|le\rangle$ ne représentent pas la même valeur. Ceci est une des contraintes les plus difficiles à rencontrer en QKD par encodage temporel, car, par exemple, des différences de températures peuvent induire des différences de longueurs de bras. La solution la plus simple à ce problème est de faires des MZI le plus petit possible, car, plus petits ils sont, moins ils sont susceptibles à des dilatations thermiques et aux différences de fabrication [15].

2.7 Performances des systèmes QKD dans la littérature

Les performances du QKD ont beaucoup évolué au fil des années. Malgré qu'il soit possible de transmettre sur des fibres optiques jusqu'à 400 km [63] de distance, le plus intéressant est de transmettre via l'air libre si l'objectif est de faire un système QKD intercontinental. En effet, transmettre dans l'air ou le vide permet de communiquer potentiellement avec des satellites, mais présente le défi d'avoir potentiellement plus de bruit à mitiger [11] [35] [46]. Une expérience a été capable de faire de la distribution quantique de clés sur une distance de 144 km dans l'air libre [57]. Donc, même si la communication terre-satellite souffre de la turbulence atmosphérique, c'est une solution prometteuse pour un internet quantique globale.

De grandes communautés en Europe [1] et des gouvernements comme la Chine [62] développent présentement leurs technologies de communication quantique. La Chine a même un satellite en orbite avec lequel ils ont fait des échanges de clés [36]. De plus, il y a aussi plusieurs compagnies comme *Id Quantique* qui font des systèmes QKD complets [41]. Bref, le QKD est en croissance et il y a plusieurs défis technologiques à relever. La simple question du choix de détecteur à utiliser reste encore à débattre. Les vitesses de transmission ne sont pas encore assez grandes pour faire compétition avec les modes de transmissions classiques. Il faut donc un receveur QKD capable d'atteindre de nouveaux sommets.

Plus spéficiquement pour le QKD par encodage temporel, plusieurs dans la communauté favorisent les systèmes plus compacts [41, 61]. La majorité vise une application en télécommunication, donc les priorités pour eux sont: opérations en 1300-1550 nm fibre et robustesse du signal (peu de perte). C'est pour ces raisons que la photonique sur silicium est une solution souvent proposée pour le QKD par encodage temporel. Ils ont accès à des photodetecteurs sensibles dans l'infrarouge et peuvent avoir des interféromètres très petits intégrés dans le silicium. Ces interféromètres petits, comme dit précédemment, sont avantageux pour générer des séparations temporelles plus proches, et donc, un canal quantique plus stable. Or, même si les séparations temporelles générées peuvent être très proches grâce aux MZI en photonique sur silicium, le détecteur devient le facteur limitant. Souvent, la communauté utilise des détecteurs externes pour ceci. La solution proposée dans ce projet est complémentaire à celle de photonique sur silicium: malgré qu'elle n'est que peu sensible à la longueur d'onde optimale, elle est potentiellement plus compacte et avec plus de traitement intégré. Comme ceci est un prototype, des aspects comme la longueur d'onde peuvent être optimisés dans de prochaines itérations.

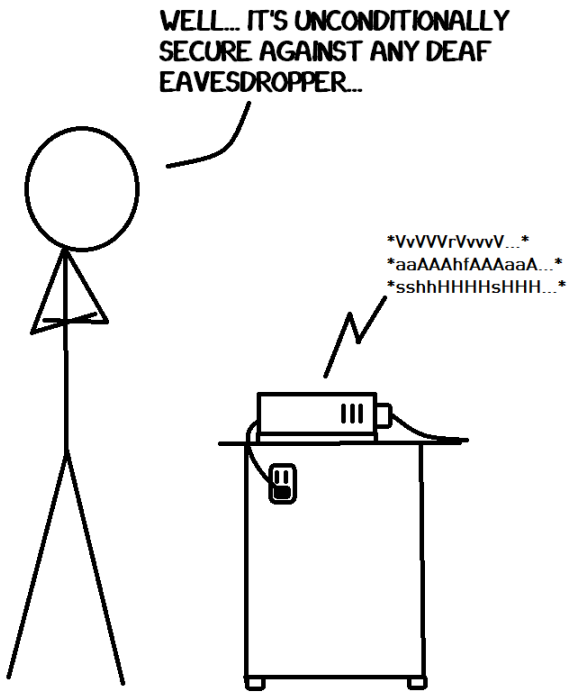

FIGURE 2.3 Petite anecdote: lorsque Bennett et Brassard on développés le premier système fonctionnel de QKD, la machine était si bruyante et changeait de son en fonction du mode de polarisation choisi, que le système était dit sécuritaire contre tout malfaiteur sourd...

CHAPITRE 3

PROBLÉMATIQUE, QUESTION DE RECHERCHE ET OBJECTIFS

L'objectif en cryptographie dans les prochaines décennies sera d'établir un réseau intercontinental de distribution quantique de clés (QKD) et les satellites QKD semblent être la solution la plus viable en ce moment. Pour y arriver, il faudra améliorer les performances de systèmes en air libre. La Chine a déjà un satellite et le Canada va suivre prochainement. Par contre, avoir un satellite n'est qu'une des étapes vers un réseau: il faut trouver des solutions aux obstacles de la transmission en air libre. L'encodage temporel permet d'éviter les problèmes de maintien de la polarisation, notamment avec un satellite dont la position et l'angle d'observation changent. L'encodage temporel est donc une technique prometteuse pour le QKD en air libre avec turbulence.

Ce problème de turbulence est encore plus important considérant que seulement un photon (qubit) est transmis à la fois. Chaque photon qui se rend au détecteur est précieux et il ne faut pas le manquer. C'est pour cela que le choix de détecteur est très important. En effet, il faut absolument que le détecteur soit monophotonique et, si c'est une matrice de détecteurs, qu'il y ait le moins d'espace mort possible entre chacun (fill factor). De plus, si l'encodage temporel est utilisé, l'horodatage doit être précis. Pour ce faire, il faut de l'électronique numérique efficace pour lire et contrôler ces photodétecteurs. Encore plus, il faut que cet horodatage se fasse le plus rapidement possible afin de minimiser le temps mort du détecteur et augmenter le taux de transmission de photons. Bref, la distribution quantique de clés avec un encodage temporel a des besoins en performances précis: un détecteur monophotonique et de l'électronique de contrôle rapide et précis. Cela fait plusieurs années maintenant que le groupe de recherche GRAMS travaille sur des PDC (Photon-to-Digital Converter) qui remplissent ces critères. La question de recherche devient:

> *Quelle est l'implémentation microélectronique d'un circuit permettant la réception de qubits photoniques encodés temporellement ?*

Répondre à cette question permettra possiblement de faire une nouvelle génération de receveurs QKD plus compacts et plus rapides. Il y a un objectif principal à ce projet et plusieurs secondaires qui découlent de celui-ci:

Primaire:

1. Concevoir et implémenter un PDC pour le receveur QKD par encodage temporel (time-bin). Cette puce devra être capable de déterminer avec assez de précision (100-50 ps) le temps d'arrivée du photon. Elle devra aussi être capable de catégoriser la valeur du qubit ($|ee\rangle$, $|el\rangle/|le\rangle$ ou $|ll\rangle$) afin de réduire la quantité de données à sortir de la puce.

Secondaire:

1. Choisir quelles parties de l'algorithme de transmission de clés est dans la puce, le FPGA, et l'ordinateur.
2. Implémenter des algorithmes spécialisés intra puce + FPGA pour l'échange de clés.
3. Faire le logiciel embarqué pour le contrôle du système (FPGA + puce).
4. Valider le receveur aux laboratoires optiques de Waterloo.

CHAPITRE 4

CONCEPTION

4.1 Survol du détecteur

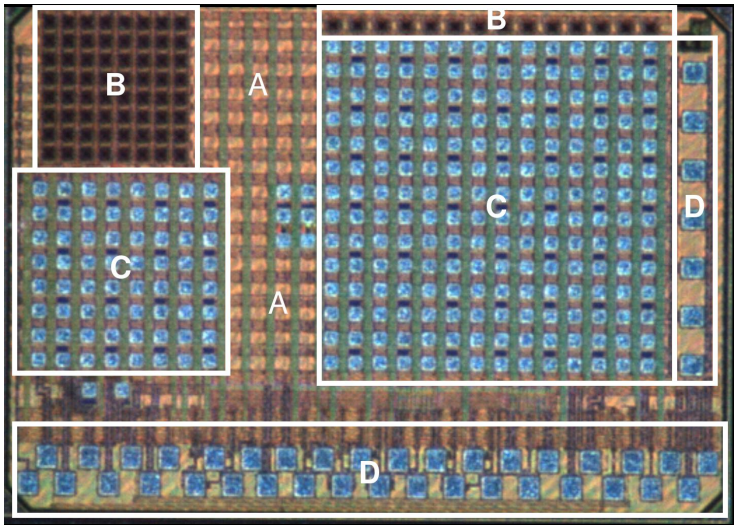

FIGURE 4.1 Image de la puce *ICYSHSR1* avec les composantes principales encadrées: registres (A), SPAD (B), TDC (C) et plots de microsoudure (D).

Pour répondre à la question de la problématique, la puce ICYSHR1, conçue et développée par une équipe et illustrée à la figure 4.1, vise à répondre à la question de la problématique. Elle est composée de 2 matrices de TDC (8×8 et 14×14), 1 matrice 8×8 de SPADs et une ligne de 14 SPADs (voir Figure 4.1). La puce mesure environ 1.2×2 mm. Les éléments spécifiquement conçus pour répondre à la problématique sont: la matrice 8×8 de SPADs, le fenêtrage des TDC (TDC Gating), le traitement de catégorisation temporelle dans la puce et le circuit de détection d'attaque par contrôle de détecteur (DCA). Les 3 premières composantes sont présentées en détail dans l'article au chapitre 7. Le circuit de détection DCA est présenté à la sous-section 4.2.4.

4.2 Présentation des sous-composantes principales

4.2.1 TDC

Le TDC (Time-to-Digital Converter) est le chronomètre qui indique le temps d'arrivé du photon entrant. C'est le coeur de *ICYSHSR1* et un facteur distinctif de notre détecteur par rapport à une caméra classique. Dans le détecteur, pour chaque groupe de 4 SPAD (2×2)

il y a un TDC. Il y a un arbitre qui détermine quel SPAD a fait feu en premier si jamais plusieurs s'activent en même temps. L'objectif étant de réduire le bruit en mode commun généré par les oscillateurs dans les TDC, cette architecture 1:4 est utilisée due aux recommandations présentées dans [44]. Une discussion sur ce sujet est présentée dans l'article (Section 7). Pour plus de détails concernant le fonctionnement des TDC, consultez les mémoires de Nicolas Roy [52], Frédéric Nolet [42] (disponible sur Savoir UdeS) et les travaux de Michel Labrecque-Dias.

4.2.2 Fenêtrage de TDC

Le fenêtrage de TDC est un circuit qui permet d'éliminer des évènements (photons) en fonction de leur temps d'arrivée. Une fenêtre d'intérêt est définie et si l'évènement arrive à l'extérieur de cette fenêtre, l'événement est éliminé et le TDC est réinitialisé afin d'être prêt pour un nouvel évènement. Toutefois, si un évènement arrive à l'intérieur de la fenêtre, l'estampille temporelle est mesurée entre le temps de déclenchement causé par le photon et la fin de la fenêtre. Ceci donne donc des estampilles temporelles relatives à la fenêtre. Pour plus de détails concernant le fenêtrage de TDC, référerez-vous à l'article au chapitre 7. La figure 7.4 illustre comment l'estampille temporelle est relative à la fenêtre.

4.2.3 Matrice de SPAD

La matrice de SPAD 8×8 en 65 nm est la composante photosensible du détecteur. Il est aussi possible de connecter des SPAD externes via les plots de connexion. Sauf si indiqué autrement, ce sont toujours les SPAD de la matrice 8×8 qui seront utilisés. Les SPAD en 65 nm ont une bonne résolution temporelle, mais souffrent de basse sensibilité (7% à 410 nm) et haut bruit (680 kHz en moyenne). Comme *ICYSHSR1* est un prototype et les SPAD sont mises en attendant le développement de SPAD intégrés en 3D, ces SPAD suffisent pour les objectifs désirés. Son haut taux de bruit (650 KHz) ne permet pas l'opération de la puce avec une source de photons uniques. Cependant, pour démontrer les fonctionnalités de la puce (estampilles temporelles et catégorisation temporelle de valeur de qubits), l'utilisation d'une source plus puissante (plus que juste 1 photon par impulsion) est acceptable. Ceci est parce que nous ne cherchons pas à démontrer la sécurité du système QKD, mais bien juste les fonctionnalités de base.

4.2.4 Circuit de détection d'attaque par contrôle de détecteur

Une attaque quantique par contrôle de détecteur (DCA) est une technique par laquelle Eve contrôle le comportement du détecteur receveur de Bob. Pour un SPAD typique, quand un photon cause une avalanche, le SPAD passe du mode Geiger au mode linéaire. En mode linéaire, il n'est plus un détecteur monophotonique et doit être "rechargé" pour revenir au mode Geiger. La technique fonctionne en aveuglant le détecteur et en le gardant

dans un mode linéaire d'opération. Dans ce mode, il devient possible de contrôler quand le détecteur perçoit un évènement, ou, plus spécifiquement, l'arrivée d'un qubit.

Le circuit DCA a été implémenté afin de détecter cette forme d'attaque. Il fonctionne en vérifiant que le SPAD n'excède pas un certain seuil de nombre de cycle de recharge. En effet, si le SPAD prend trop de cycles pour se recharger après un évènement, c'est un signe que le SPAD est aveuglé. Le scénario que le SPAD soit aveuglé durant l'opération est un comportement qui ne devrait pas avoir lieu. Dans ce cas, un signal d'alarme est levé et l'utilisateur (Bob) est averti de l'état compromis de ses détecteurs. Il a est à noter qu'un détecteur normal ne serait pas en mesure d'avertir l'utilisateur. Ceci est dû au fait que comme le détecteur est aveuglé, il ne sort pas de données. Du point de vue du détecteur ordinaire, il n'y a simplement pas de photon entrant. C'est ici que le circuit DCA fait la différence: il est capable de déterminer la différence entre un aveuglement ou simplement aucun photon entrant.

4.2.5 Estampille temporelle absolue QKD (*Absolute timestamp QKD*) et estampille temporelle relative QKD (*Relative timestamp QKD*)

Les données sortantes des TDC doivent être traitées afin d'avoir une estampille temporelle en picoseconde. Cette opération de conversion fait partie de la liste d'opération post-traitement qui peut être faite dans la puce. Pour plus de détails concernant les détails de cette opération, référez-vous au mémoire de Pascal Gendron [22].

Pour les travaux présentés dans ce mémoire, comprendre la différence entre l'estampille temporelle absolue et relative est suffisant. L'estampille temporelle absolue est en référence à l'horloge du système et l'estampille temporelle relative est en référence à la fin du fenêtrage du TDC (section 4.2.2). L'estampille temporelle relative a été ajoutée à la puce spécialement pour le QKD afin de pouvoir catégoriser le temps d'arrivée du photon à l'intérieur de la fenêtre par un code temporel sans transmettre toute l'information de l'estampille temporelle. Pour plus des détails concernant ces modes de post-traitement référerez-vous à l'article au chapitre 7.

4.2.6 Trame de communication

La communication avec la puce *ICYSHSR1* se fait via 2 lignes de transmission série à 250 Mb/s. La première ligne sert à transmettre les commandes vers la puce et la deuxième sert à sortir les réponses de commandes et les données. Le format des données sortantes est toujours en paquets de 64 bits et peut varier en fonction du mode de post-traitement choisi dans la configuration de la puce. Peu importe le format, le paquet de données est

long de 64 bits. Ceci est une limitation du système, car certains formats (spécialement pour le QKD), n'ont pas besoin de 64 bits par trame. Avoir une longueur de trame plus flexible pourrait être une optimisation facile pour une prochaine version de la puce dédiée au QKD. En effet, pour le QKD, un des facteurs limitants est la sortie des données de la puce basse vitesse (250 MHz) et la taille fixée à 64 bits qui est trop grande. Pour plus de détails concernant le format des données référerez-vous à l'article au chapitre 7. L'horloge système de 250 MHz de la puce est utilisée par le FPGA pour transmettre les données en phase. Dans le passé, cette même horloge était utilisée par le FPGA pour la réception de données. L'inconvénient de ceci était que la réception de données n'était pas toujours en phase. Pour cette raison, pour la puce *ICYSHSR1*, l'horloge est retransmise par la puce vers le FPGA avec la ligne série de données. Ceci assure que l'horloge et les données soient pratiquement toujours en phase.

CHAPITRE 5

MÉTHODE ET CARACTÉRISATION

5.1 Tests électroniques des TDC

Il y a deux types de tests électroniques principaux pour la caractérisation des TDC: corrélés et non corrélés. Dans les tests corrélés, le signal de départ et d'arrêt des TDC proviennent de signaux contrôlés en temps (délai et phase fixe par rapport à une horloge de référence). Dans les tests non corrélés, au moins un des signaux de départs ou d'arrêt provient d'une référence connue (souvent le signal d'arrêt) alors que l'autre provient d'un autre oscillateur, voire d'un SPAD (souvent le signal de départ). Donc, dans le cas non corrélé, le délai de temps mesuré par les TDC est aléatoire. Pour tous les tests corrélés, la fin de la fenêtre (déclenchée par un signal externe) est utilisée comme "stop" pour les TDC. Ceci fait en sorte que des signaux externes peuvent agir comme les "start" et "stop" des TDC. Les méthodes de tests corrélés et non corrélés ont été utilisées plusieurs fois dans le groupe (voir les mémoires de Nicolas Roy [52] et Frédéric Nolet [42]) et sont bien documentés. Pour plus de détails concernant les tests électroniques utilisant la fenêtre dans *ICYSHSR1*, référerez-vous à l'article au chapitre 7.

5.2 Tests optiques

Il y avait plusieurs bancs de tests optiques utilisés pour différentes mesures. Notamment, certains tests ont été faits à l'Université de Waterloo. Pour plus de détails concernant les bancs de tests optiques référerez-vous à l'article au chapitre 7.

5.3 Acquisition de données

5.3.1 Les PCBs du système d'acquisition

Le système d'acquisition est composé de 3 PCB principaux: ZCU102, PCB «devkit» (*adapter board*) et PBC «head» (*head board*) (voir figure 5.1). Le ZCU102 est un PCB avec un FPGA ZYNQ-UltraScale de Xilinx. Il est connecté au devkit via un connecteur en mezzanine. Ce devkit contient tous les circuits de contrôle pour l'ASIC et les circuits nécessaires pour les tests électroniques. Le devkit est connecté par câble SAMTEC à la head qui contient des répéteurs, des régulateurs de tension et la puce qui y est microsoudée. Pour des tests optiques, on ajoute un support de lentille afin de focaliser la lumière sur la matrice de SPAD (voir figure 5.2). Les 3 PCB (surtout le devkit) doivent gérer 3 signaux essentiels

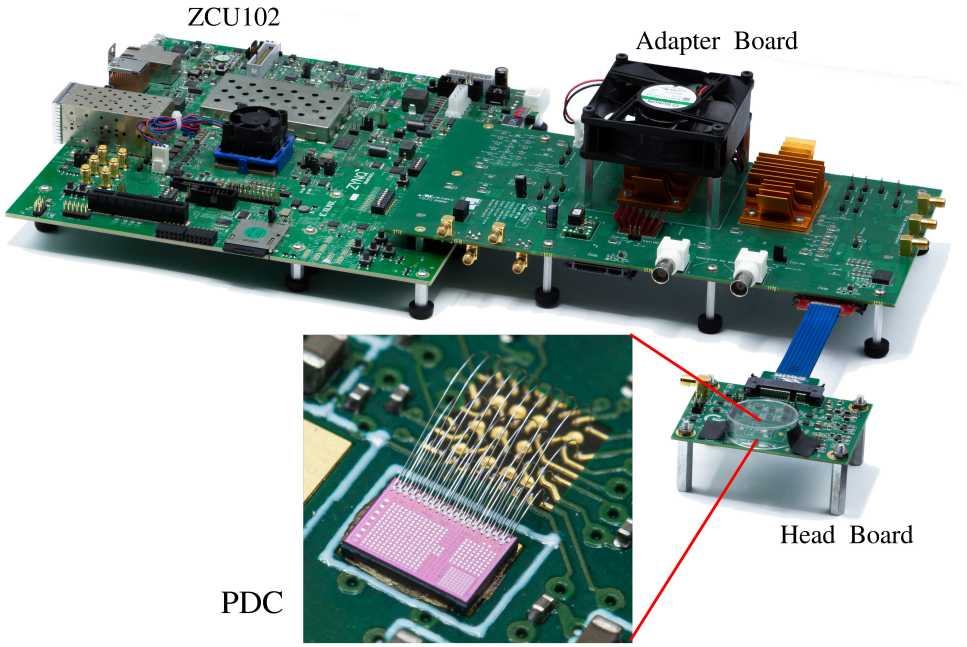

FIGURE 5.1 Les 3 PCB qui composent le système d'acquisition et de contrôle pour la puce *ICYSHSR1*. Le PDC est la puce *ICYSHSR1*.

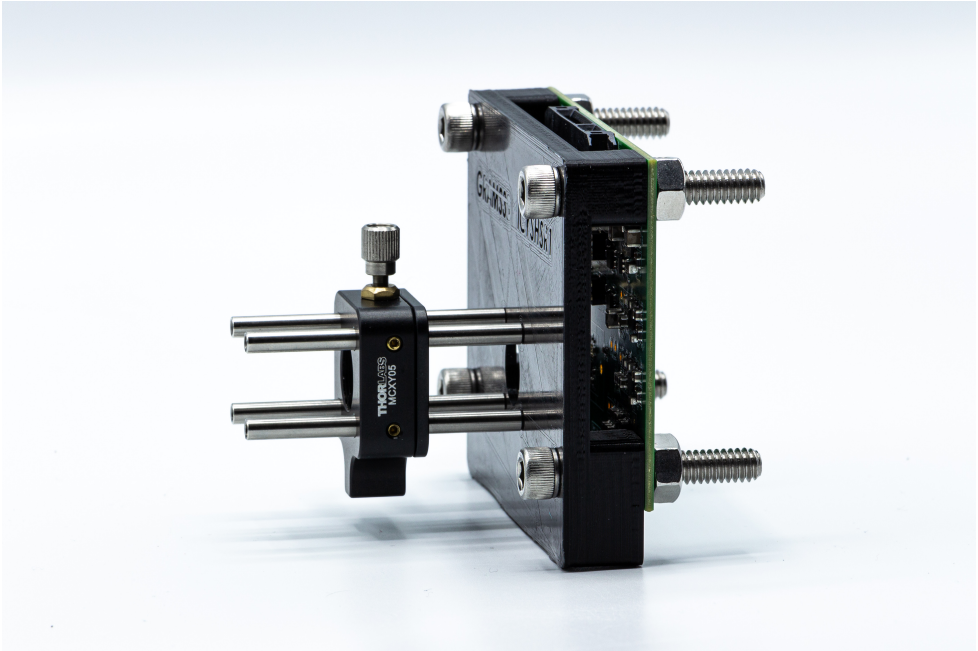

FIGURE 5.2 Image du PCB head avec le support à lentille.

au fonctionnement et à la validation de la puce *ICYSHSR1*: une horloge à 250 MHz, le signal de "start" et le signal de fenêtre. L'horloge à 250 MHz est l'horloge système de la puce. Le signal de "start" est celui qui déclenche le départ des TDC. Finalement, le signal de fenêtre déclenche le début de la fenêtre à l'intérieur de la puce. Le devkit génère ou

ajuste ces signaux, le ZCU102 contrôle comment le devkit génère et achemine ces signaux et le PCB «head» assure le bon fonctionnement de la puce et s'assure que les signaux respectent l'interface électronique de celle-ci.

5.3.2 Contrôle et tests automatiques

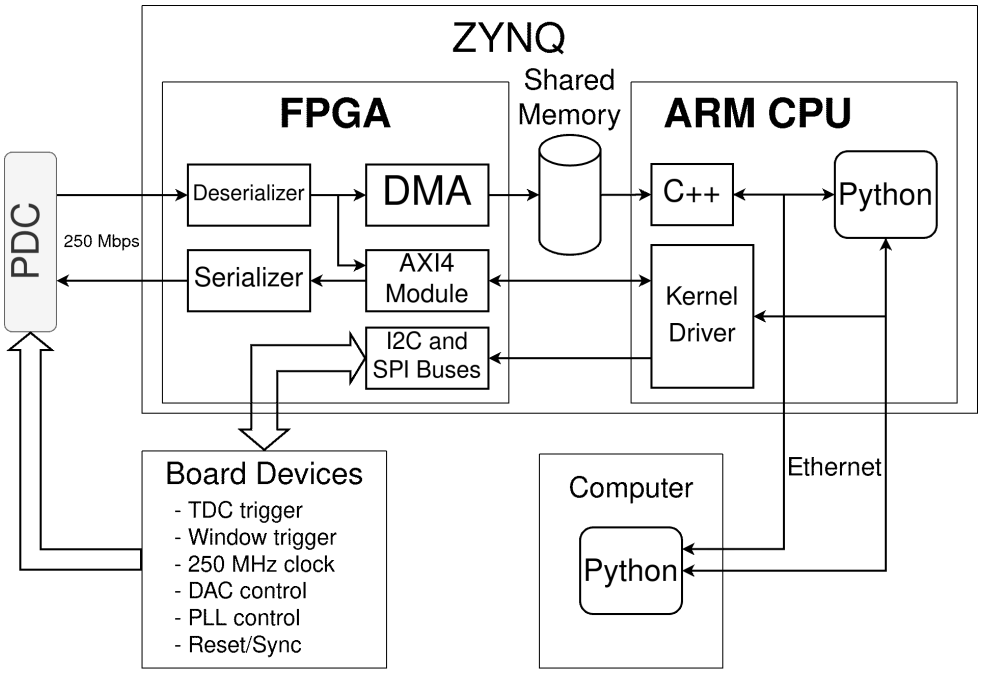

FIGURE 5.3 Schéma du flux des données de la puce et des commandes de contrôle vers la puce. Le FPGA ZYNQ sur le ZCU102 agit comme le coeur de contrôle.

Schéma de contrôle et de parcours de données Le FPGA ZYNQ contient un CPU ARM qui exécute Linux. Ce CPU agit comme centre de contrôle de tout le système et facilite l'automatisation de tests. On peut se connecter à distance au système et faire des tests électroniques. Le ZYNQ contrôle les composantes du devkit. La figure 5.3 montre les composantes de contrôle et le déplacement des données dans la puce (PDC) et jusqu'à l'ordinateur. La section FPGA est conçue avec le logiciel Vivado. La DMA (Direct Memory Access) permet de placer les données entrantes (venant du PDC) dans un bloc de mémoire qui est accessible par le CPU (et donc Linux et l'utilisateur). Le module AXI4 permet de formater les commandes vers le *ICYSHSR1* et d'attraper les réponses des commandes sans que l'utilisateur ait besoin de se soucier des détails de la communication. Le FPGA agit aussi comme un pont de communication avec les autres composantes (oscillateurs, diviseur d'horloge, mux, etc.) dans le PCB devkit.

Scripts Python pour le contrôle des ASIC Python est le langage de script d'automatisation principal. Il est possible d'exécuter des scripts Python directement sur le ZYNQ ou d'exécuter les scripts à distance. Cette flexibilité rend le système très modulaire. Par exemple, une interface graphique pour les tests optiques en laboratoire à été relativement facilement réalisée grâce à ces scripts Python. De plus, il est possible d'enregistrer les données brutes venant de la puce sur le PCB ZCU102 même ou sur un ordinateur connecté.

CHAPITRE 6

RÉSULTATS

6.1 TDC

Les résultats électroniques consistent principalement en des mesures de performances des TDC. La gigue temporelle et la résolution sont les deux valeurs les plus importantes pour un TDC. Dans les résultats qui suivent, “Matrice 1” réfère à la matrice 4×4 de TDC utilisé pour l’application de QKD. De plus, les résultats de TDC sont séparés en PLL et DAC. Ceci est dû au fait que les TDC peuvent être asservis via les PLL internes ou des DAC externes. Pour plus de détails concernant les PLL, référez-vous aux travaux de maîtrise de Michel Labrecque-Dias. Dans les figures qui suivent, je présente les gigues temporelles et les résolutions temporelles des TDC quand ils opèrent tous en même temps.

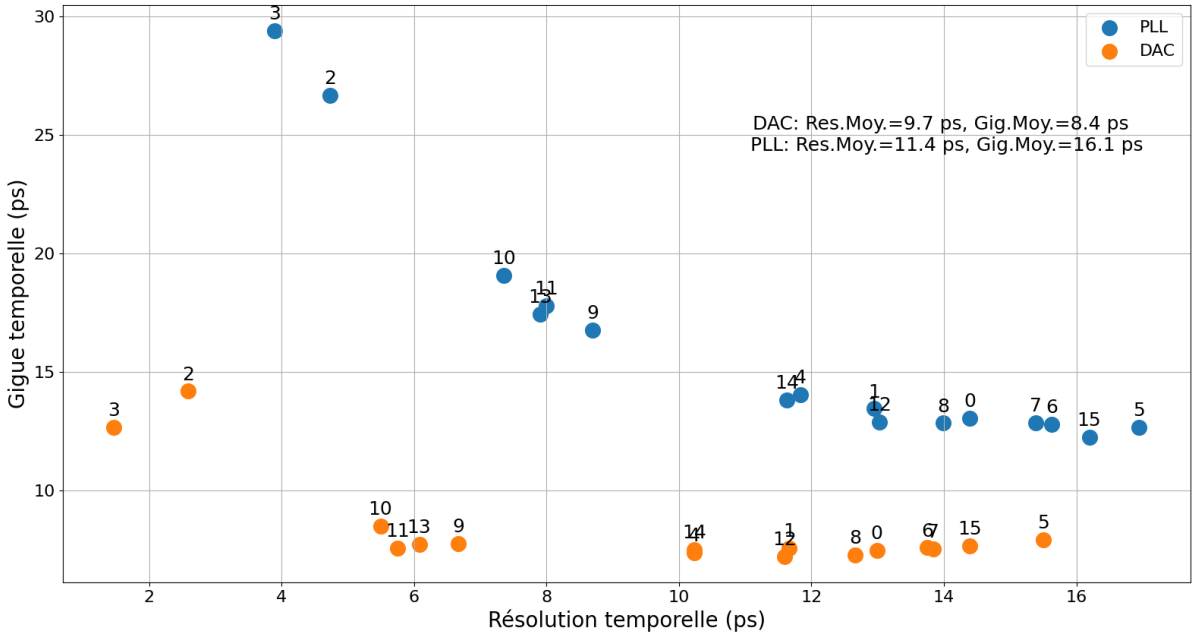

FIGURE 6.1 Gigue temporelle en fonction de la résolution des TDC asservis par PLL et DAC avec la matrice #1. Le numéro de chaque point indique le numéro du SPAD (de 0 à 15). Durant ces mesures, tous les TDC sont actifs.

Si l’on compare avec les résultats entre les deux modes de fonctionnement (DAC et PLL) présenté à la figure 6.1, la différence principale est du côté de la gigue temporelle. En effet, pour des résolutions similaires dans les 2 scénarios, la moyenne des gigues temporelles

passe de 16.1 ps (avec PLL) à 8.4 ps (avec DAC). Il est incertain pourquoi la performance en matrice est 2 fois meilleure avec les DAC versus les PLL, mais des sources possibles sont présentés dans la discussion. Parce que les résultats avec les DAC étaient meilleurs, les mesures suivantes sont faites en utilisant les DAC.

6.1.1 Fenêtrage de TDC (DAC seulement)

Le circuit de fenêtrage de TDC réinitialise le TDC dépendant si un évènement arrive à l'intérieur d'une fenêtre d'intérêt. C'est donc un circuit qui dépend beaucoup du circuit générateur de fenêtres fait par Pascal Gendron. Je reprends ici les résultats du mémoire de mémoire de Pascal Gendron [22] portant sur le générateur de fenêtre afin de contextualiser les résultats du circuit de fenêtrage de TDC. Pour plus de résultats concernant le fenêtrage de TDC, référerez-vous à l'article au chapitre 7.

Décalage temporel

Les résultats présentés à la figure 6.2 démontrent que la fenêtre est ajustable entre environ 100 ps et 7000 ps. De plus, la propagation du signal de fenêtre à travers la matrice engendre un décalage (communément appelé «skew») lié à la position dans la matrice d'au maximum 50 ps (figure 6.3). Parce qu'il est possible de compenser ces décalages fixes pour chaque TDC, cette matrice de décalages n'est pas un obstacle au fonctionnement du détecteur. Donc, pour résumer, ces résultats indiquent que le circuit de fenêtrage de TDC sera limité entre 100 ps et 7000 ps. De plus, il faudra tenir compte du décalage de l'ordre de 50 ps. Tout ceci est considéré dans les mesures. Par exemple, la figure 6.7 présente des données avec une fenêtre de 1500 ps et prends en considération le décalage.

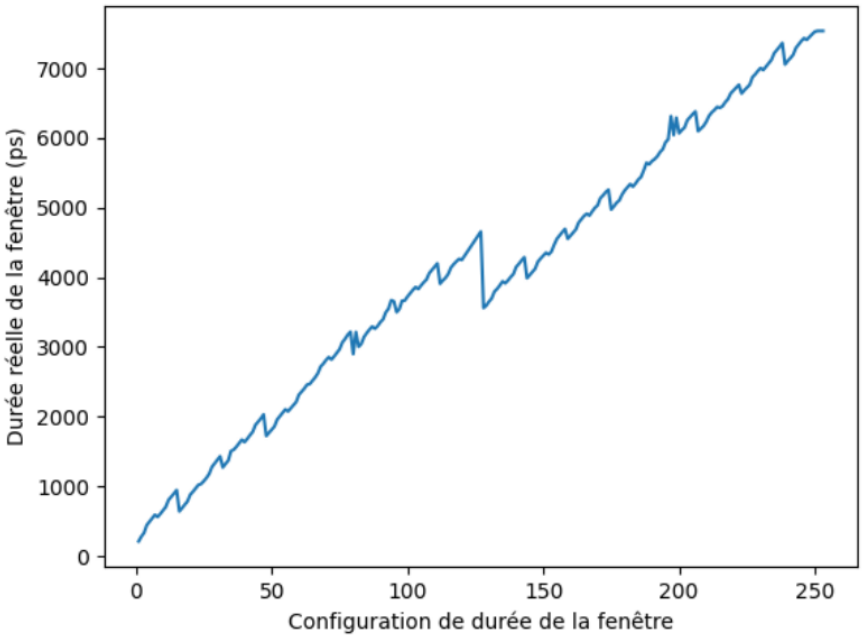

FIGURE 6.2 Largeur de la fenêtre aux pixels (après distribution au travers de la matrice) en ps selon le code de configuration choisi. Figure tirée du mémoire de Pascal Gendron [22] (disponible sur Savoir UdeS).

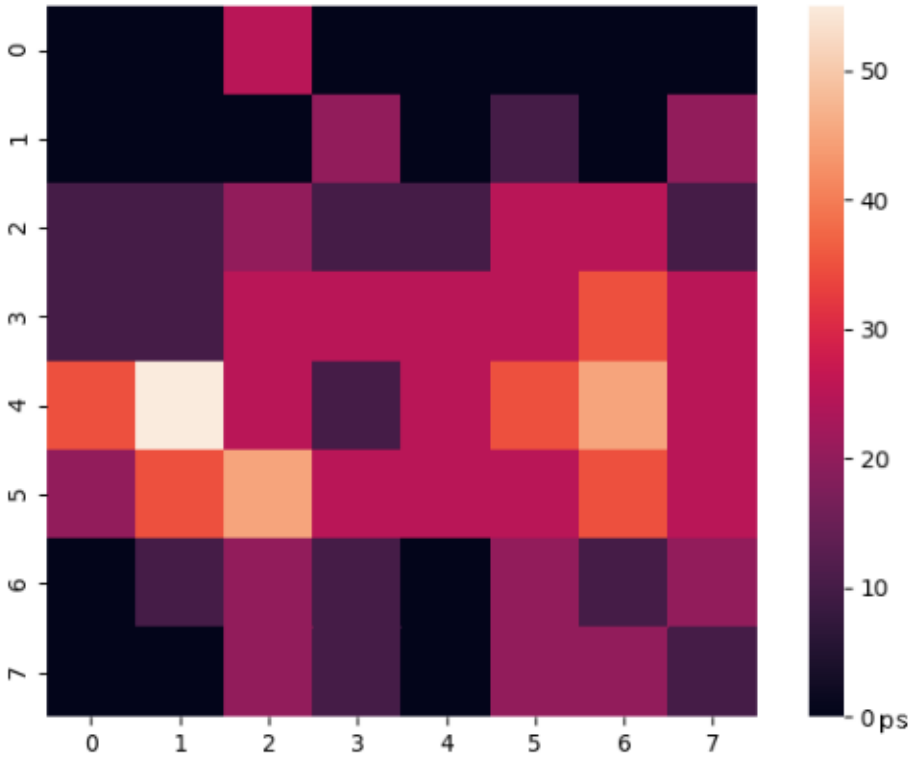

FIGURE 6.3 Décalage temporel relatif entre le moment de réception du signal de fenêtre pour les différents pixels de la matrice 8×8 (en ps). Figure tirée du mémoire de Pascal Gendron [22] (disponible sur Savoir UdeS).

6.2 Résultats de mesures optiques

Pour l'application de QKD, il est possible d'utiliser un receveur avec juste 1 pixel. Toutefois, avoir plusieurs pixels offre les avantages d'avoir une plus grande surface photosensible, facilite l'alignement avec l'émetteur et de diminuer le temps mort effectif du détecteur. Donc, il est désirable de pouvoir utiliser tous les pixels en même temps. Or, cela ajoute plus de complexité qui deviendra apparente au cours de cette section. C'est pour cette raison que l'article au chapitre 7 présente les résultats en utilisant juste 1 pixel pour le QKD. Dans cette section, des résultats complémentaires sont présentés ainsi que les résultats d'estampilles temporelles de photons en utilisant tous les pixels. Les résultats en utilisant tous les pixels ne sont pas ceux espérés. Or, comme ce n'était pas essentiel pour le QKD, l'investigation sur les performances moins bonnes a été limitée. Les résultats sont présentés afin de proposer les pistes potentielles de recherche future.

6.2.1 Matrice de SPAD 8×8

Bruit thermique

Le bruit thermique (Dark Count Rate en anglais, DRC) est le taux d'évènements mesuré sans illumination. Ce sont des évènements causés par excitation thermique à l'intérieur des SPAD (d'où le nom de bruit thermique). La figure 6.4 montre le bruit thermique de chaque SPAD avec une moyenne de 680 kHz. Pour un détecteur monophotonique, cette

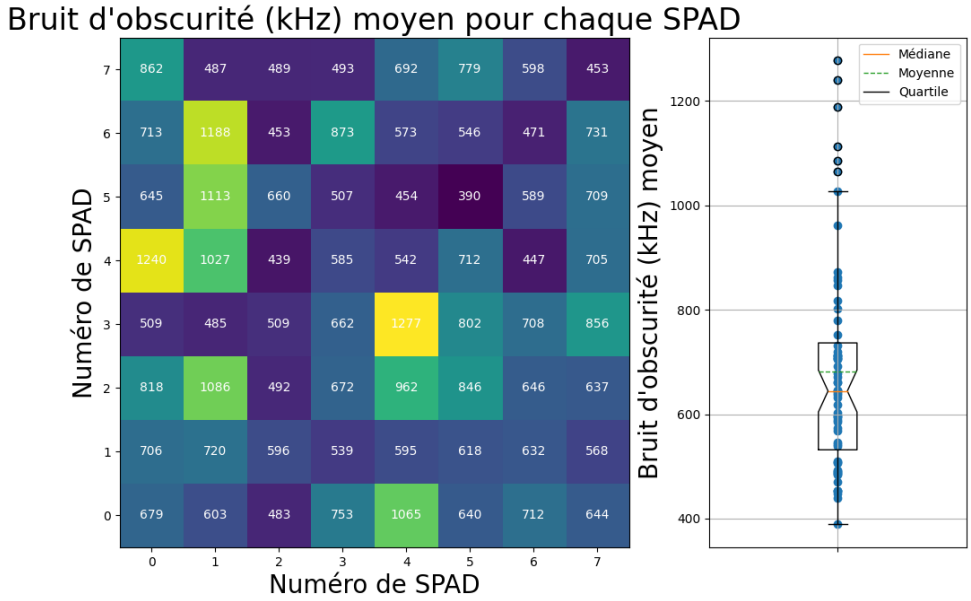

FIGURE 6.4 Bruit d'obscurité (thermique) des SPAD 65 nm en kHz. La moyenne est d'environ 680 kHz.

valeur est haute si on compare au tableau 2.7 de Hadfield. Comme dit précédemment, ce

détecteur est un prototype qui a pour but de démontrer ses fonctionnalités QKD donc ce haut bruit thermique est acceptable. Il ne semble pas avoir de dépendance entre le bruit et la position du SPAD dans la matrice.

Résolution temporelle avec la lumière focalisée sur un pixel

La résolution temporelle est rapportée dans l'article à la figure 7.16 (chapitre 7).

Décalage interpixel

Le décalage interpixel est important à caractériser afin de le corriger et d'avoir un système qui mesure un temps juste, peu importe le pixel choisi. En d'autres mots, tous les pixels doivent avoir le même référentiel de temps, idéalement, sans décalage. Dans la situation où les pixels n'ont pas de décalages relatifs, il devient possible pour le QKD d'exploiter la matrice de pixel au complet. En effet, si les qubits (photons) sont tous focalisés sur un pixel, le receveur QKD fonctionne, mais il sera limité par le temps mort du pixel. Par contre, si la lumière est répartie sur la matrice de pixel, pour le même flux de qubits, le temps mort effectif du détecteur diminue. Par contre, si le référentiel de temps entre chaque pixel souffre de décalages, les pixels donneront des valeurs d'encodage temporel différent. C'est pour cette raison qu'il est désirable de minimiser le décalage interpixel.

Contrairement aux mesures de décalages présentés à la figure 6.3, qui ne concerne que le décalage au travers de la matrice du signal de fenêtre, cette section présente le décalage de chaque SPAD (pixel). Par exemple, si le SPAD 0 s'active en même temps que le SPAD 1, il y aura un décalage entre les deux SPAD. Pour cette mesure, un laser pulsé corrélé est focalisé sur 1 SPAD à la fois et un histogramme des estampilles temporelles est généré pour chaque SPAD. Chaque histogramme contient un sommet avec le plus de comptes (le mode) et ce sommet est considéré le décalage moyen de ce SPAD. Le décalage est trouvé en prenant note d'où le sommet de la gaussienne se situait (similaire à la figure 6.7). La différence entre chaque sommet de décalage correspond aux décalages interpixels. Ceci donne donc les différences de décalage entre chaque pixel. L'essentiel à retenir est que la distribution de décalage est similaire entre les deux mesures. Par exemple, les SPAD avec un petit décalage dans la mesure (a) ont aussi un petit décalage dans la mesure (b) dans la figure 6.5. De plus, la différence de décalage à l'intérieur de la matrice pouvait atteindre jusqu'à 120 ps.

La mesure a été répétée deux fois parce que certaines mesures ne concordaient pas en laboratoire. La figure 6.5 montre les valeurs mesurées pour chaque SPAD lors des 2 mesures et figure 6.6 illustre les différences. En moyenne, les délais sont similaires entre les deux mesures (une différence moyenne de 0), mais les décalages pouvaient fluctuer de +/- 30 ps d'une mesure à l'autre. La source de cette différence n'est pas connue et comme ce résultat

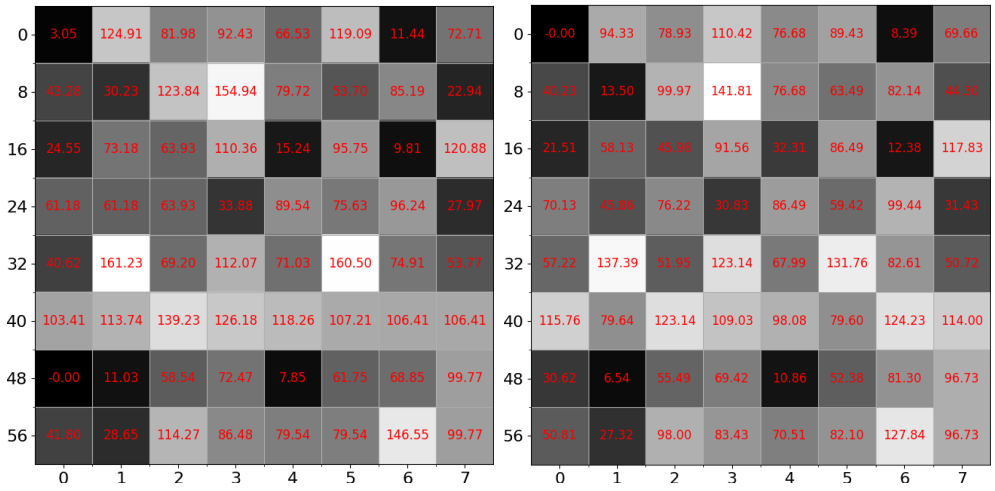

FIGURE 6.5 Mesure de décalage temporel entre chaque pixel. A priori, mesure 1 (a) et mesure 2 (b) sont équivalentes. Les deux mesures de décalage prises pour chaque SPAD dans la matrice 8×8. Pour les deux matrices, le plus petit décalage est soustrait à toute la matrice. Ceci donne donc les différences de délais entre chaque pixel. L'important à retenir est que la distribution de délais est similaire entre les deux mesures.

n'est pas essentiel au fonctionnement de la puce en mode QKD, cette question n'a pas pu être autant explorée que voulu dû aux limitations de temps. Toutefois, 2 explications potentielles seront présentées ici afin d'aider des travaux futurs.

Il y aurait 2 explications possibles pour ce comportement: soit le banc de tests optiques a une faille ou des variations thermiques affectent les délais des pixels. Les 2 mesures ont été prises sur 2 jours adjacents et consistaient à orienter le faisceau laser dans chaque pixel. Il est possible que le faisceau laser parcourt un chemin légèrement différent pour chaque pixel, mais comme aucun patron dans les données ne semble indiquer ceci, la différence de chemin est jugée négligeable. De plus, 30 ps correspondent à environ 1 cm de distance pour la lumière. Il est très improbable qu'il y ait une différence de chemin de 1 cm. Ensuite, comme la température n'est pas régulée sur la puce, la température pouvait être différente entre les deux mesures. Des "points chauds" différents auraient pu faire changer le comportement temporel des SPAD ou le comportement temporel des cellules de délais et bascules (*latch*) du circuit de fenêtrage de TDC qui agissaient comme le signal d'arrêt dans ces mesures. Malgré que la moyenne reste stable, avec une différence moyenne de 1 ps (ligne pointillée verte), le décalage entre les deux mesures pouvait changer de +/- 30 ps. Les explications les plus plausibles sont un changement de délais dû à la température du système ou une erreur dans le banc de tests optiques. Comme c'est un comportement qui

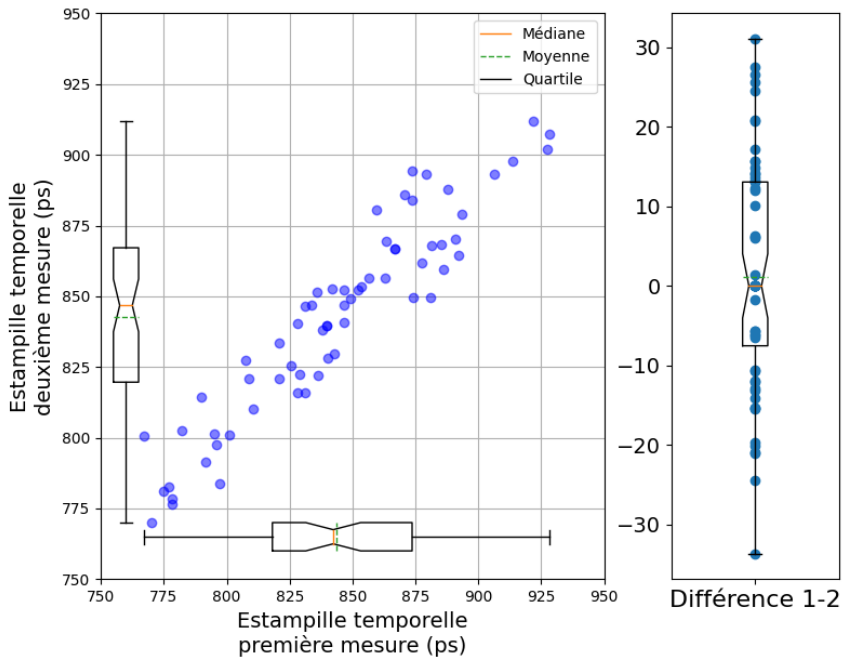

FIGURE 6.6 Comparaison des deux mesures de décalage pour la matrice de SPAD. Dans la figure de gauche, l'axe des abscisses correspond aux premières mesures et l'axe des ordonnées correspond à la deuxième mesure pour le même SPAD. S'il n'avait pas de fluctuation, les points formeraient une ligne droite. La figure de droite montre les différences entre la première et deuxième mesure.

semble aléatoire (+/- 30 ps) avec une moyenne stable (1 ps de différence en moyenne), un processus thermique semble la meilleure explication pour l'instant. Des travaux futurs pourront explorer cette question en plus de détails avec un banc de test optique conçu pour cette mesure.

Résolution temporelle avec tous les pixels

Dans cette mesure, tous les pixels sont éclairés par le laser en même temps. La figure 6.7 montre la somme de toutes les gigues temporelles des SPAD. La figure 6.7 de gauche présente l'histogramme de gigue temporelle pour tous les SPAD sans correction du décalage associé à chaque SPAD. Dans la figure 6.7 de droite, les mesures de gigue temporelle ont été corrigées pour chaque SPAD en fonction de son décalage spécifique. La correction de décalage se fait à l'intérieur de la puce avec les circuits de traitement de données.

Avec cette comparaison, l'avantage de faire l'ajustement de délai devient apparent avec la réduction de gigue temporelle totale. Dans la figure 6.7, dû au haut bruit thermique des SPAD, le bruit de fond est haut et est vu sur toute la plage du fenêtrage de TDC. De plus, comme la forme du faisceau lumineux est gaussienne, les SPAD en périphérique

obtenaient moins de photons de ceux centraux. Ceci a fait en sorte que le bruit de ces SPAD périphériques augmente le bruit de fond apparent dans la figure. 6.7

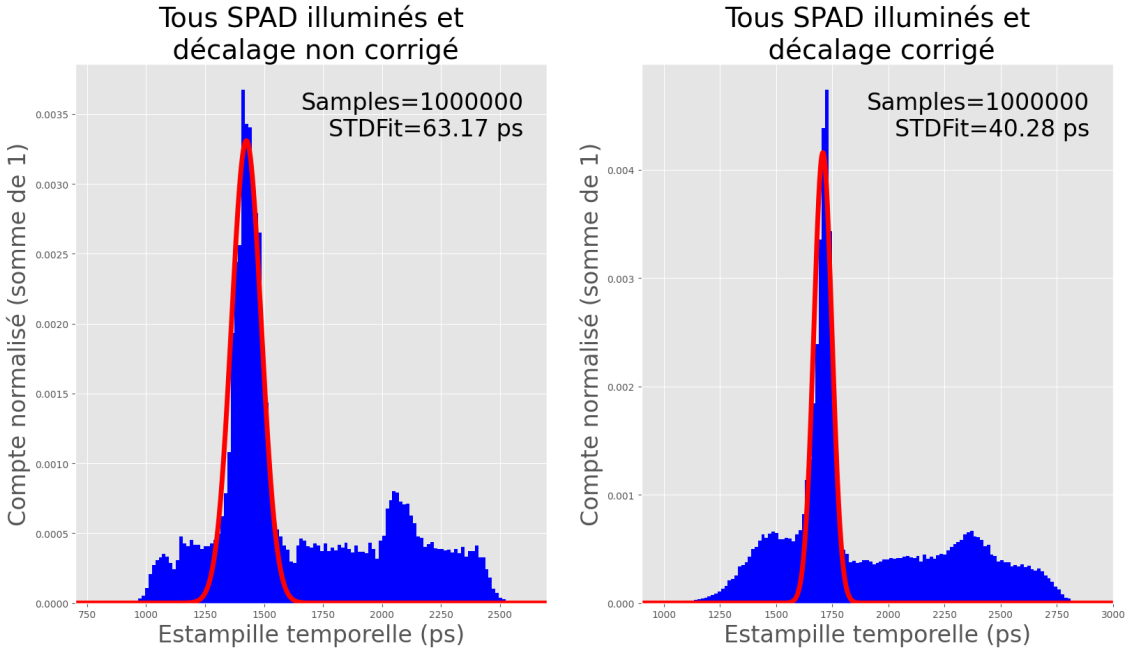

FIGURE 6.7 Comparaison entre sans et avec correction de décalage (skew) entre SPAD. Le SPTR total apparent de la somme des pixels diminue quand on fait la correction de ce décalage dans la puce. Le bruit de fond des SPAD est haut et est apparent sur toute la plage du fenêtrage de TDC (1500 ps) dans les deux figures.

CHAPITRE 7

CONVERTISSEUR PHOTON-NUMÉRIQUE (ARTICLE)

Titre original: Towards a Multi-Pixel Photon-to-Digital Converter for Time-Bin Quantum Key Distribution

Auteurs et affiliations:
Simon Carrier [1,*], Michel Labrecque-Dias[1,], Ramy Tannous[2,], Pascal Gendron[1,], Frédéric Nolet[1,], Nicolas Roy[1,], Tommy Rossignol[1,], Frédéric Vachon[1,], Samuel Parent[1,], Thomas Jennewein[2,], Serge Charlebois[1], and Jean-François Pratte[1,]

[1] Université de Sherbrooke, Québec, Canada ;

[2] Institute for Quantum Computing, Department of Physics & Astronomy, University of Waterloo ; **Date de soumission:** février 2023

Revue: MDPI Sensors

Titre français: Vers un convertisseur photon-numérique multi-pixel pour distribution quantique de clés par encodage temporel.

Contribution au document Cet article contribue au mémoire en élaborant sur les composantes, fonctionnalités et performances de *ICYSHSR1*. Il commence par une courte mise en contexte du QKD par encodage temporel suivi d'une présentation de la puce. Les composantes spécialement développées pour le QKD (fenêtrage de TDC, matrice 8×8 de SPAD et traitement de données) sont mises de l'avant. Le résultat principal de l'article est la mesure des estampilles de l'encodage temporel à travers un interféromètre Mach-Zehnder avec une résolution de 22.7 ps RMS.

Résumé francais: Des détecteurs monophotonique avec bonne précision temporelle et traitement de signal intégré sont avantageux pour les applications quantiques. Ceci est particulier vrai pour la distribution quantique de clés (QKD) en *time-bin* qui encode les qubits avec le temps et la phase. Dans les travaux présentés, un prototype convertisseur photon-numérique (PDC) en 65 nm TSMC CMOS avec traitement de signal intégré a été conçu pour ces applications quantiques. Ce PDC atteint une précision temporelle de 22.7 ps RMS et permet une séparation *time-bin* de 158 ps à 410 nm de longueur d'onde.

État de soumission L'article à été accepté et publié.

Mes contributions à l'article: Je suis le premier auteur de l'article. J'ai contribué à la

conception et au développement de la puce présentée. J'ai fait les mesures et l'analyse des résultats.

7.1 Introduction

Quantum key distribution (QKD) is a key generation and sharing protocol where the security relies on quantum properties instead of computational complexity of certain mathematical problems such as in classical cryptography [25, 50]. Typically in QKD, the qubits are photons sent from the sender to the receiver via fiber-optical networks, free-space links of space-to-ground links. Multiple methods of encoding information in single optical qubits (photons) have been developed [56, 4, 51, 23]. One of these is called "time-bin" in which the information is encoded in the time of arrival and phase of the photon, which necessitates high-precision single-photon detectors at the receiver [13].

Time-bin encoding is achieved with unbalanced Mach–Zehnder interferometers (MZI) at both the sender and receiver. These must be as identical and stable as possible to avoid any phase drifts. The sender MZI prepares the qubit in one of four states from the time and phase bases: early (E), late (L), early and late with a constructive phase difference ($\phi = 0$), and early and late with a destructive phase difference ($\phi = \pi$). The MZI receiver will detect one of four photon states: early–early (EE), late–late (LL), early–late (EL), or late–early (LE), which are temporally separated according to MZI path asymmetry.

Time-bin encoding offers advantages over polarization encoding in that it is relatively immune to depolarization and polarization mode-dispersion [29, 33] of the channel and does not require polarization frame alignment of the sender and receiver. It is important to note that reducing the time separation between time-bins offers closer E and L time-bins, which allows for a more compact and stable MZI. This is, in particular, attractive for free-space applications where the distortion of the spatial mode requires elaborate imaging interferometers [33], particularly challenging for applications under stringent volume and mass restrictions such as satellite or handheld QKD. Typically, the outputs of the single-photon detectors, such as a single-photon avalanche diode (SPAD) [9, 32] or a superconducting nanowire single-photon detector (SNSPD) [8, 61], are connected to a time-tagger, a specialized chronometer often implemented in an FPGA. However, these configurations present two challenges: they can be bulky due to cooling or device size and suffer from signal degradation, because the connection circuitry and cables could reduce timing resolution. Furthermore, a conventional QKD system is based on single-pixel single-photon detectors. However, array detectors could be very beneficial for the system performance as they can enhance the photon count rate, perform quantum signal tracking tasks, and improve resilience against blinding attacks [54].

To address these challenges, a photon-to-digital converter (PDC) prototype is developed, comprising a single-photon detector array coupled to tailored digital electronics to process

information such as the timestamp of each photon using embedded time-to-digital converters (TDC). This configuration can be realized in a very compact form (a few square millimeters for the PDC chip), and the distance between the detector and time-tagger is very short (<1 mm).

The PDC has an 8 × 8 SPAD [17, 26] array in addition to the electronics on-chip (see Figure 7.1). This implementation is suboptimal because the 65 nm SPADs, although having a good timing resolution (7.8 ps FWHM SPTR at 410 nm wavelength [43]), suffer from low photon detection efficiency (7% at 410 nm in this work) and high noise (680 kcps average per SPAD). A more optimized solution would be to use another specialized technology for the SPADs and integrate them in 3D (on top) of the 65 nm CMOS electronics [49], which is the goal of future iterations. Although the shortcomings of 2D integration and the 65 nm SPADs were acceptable to demonstrate the QKD functionalities in this prototype, this PDC was designed to allow a future 3D integration and already includes top-side bond pads.

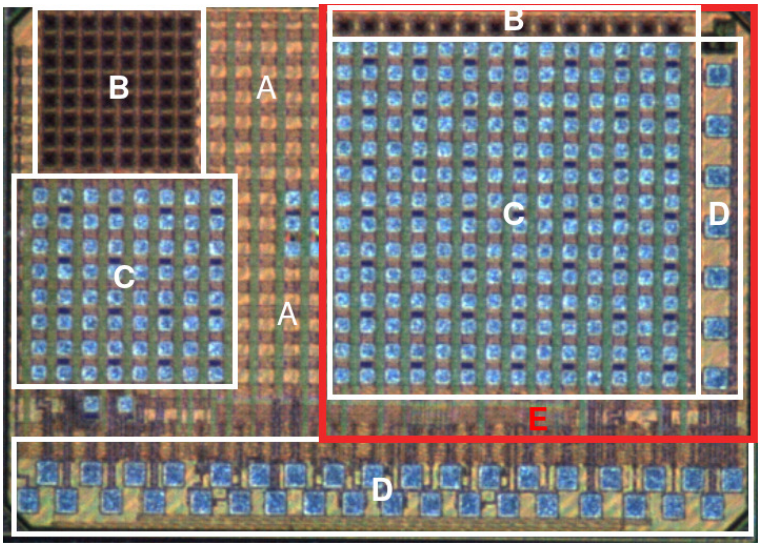

FIGURE 7.1 PDC diagram with the four main components: registers (**A**), SPADs (**B**), TDCs and quenching circuits (**C**), wirebonding pads (**D**). The rightmost array (red, **E**) was designed for another application and is not described in this paper.

In the QKD post-processing, the key exchange requires a comparison of the absolute timestamps of all received photon detections with the corresponding emission times, via communication over a classical channel. Our custom PDC design directly supports this exchange. Iterating on previous work [44], the proposed PDC includes three features specifically targeted at QKD: timing window generation, TDC gating, and custom on-chip

post-processing. The timing window generation allows the PDC to create variable-length gating signals on-chip when an external trigger is raised. It also allows the TDC to timestamp events relative to the end of the window signal. TDC gating uses the window signal to reject events outside of a window of interest. The custom on-chip processing converts the TDC code to picosecond timestamps directly and categorizes the timestamp into its time-bin value (EE, LE/EL, or LL). These added features allow the receiver's detector to directly output the time-bin value, which reduces the data-volume substantially, thereby simplifying the entire QKD post-processing. These three components will be explained in further details in the *Architecture* subsection of *Materials and Methods*. This is followed by a presentation of the testing and data acquisition setups in the *Methods and Testing Setups* subsection. The electronic and optical performance results are then presented in the *Results* section. Finally, a discussion of the results with a comparison to previous publications.

7.2 Materials and Methods

7.2.1 Architecture

PDC Structure

The PDC was designed in TSMC 65 nm LP (low power) CMOS technology, with the goal to have the SPAD array integrated in 3D (on top) of the electronics. The 65 nm technology was chosen because it is small enough that it permits the TDCs and other circuits to fit in the restricted volume beneath each of the SPADs for 3D integration. This meant taking into account the footprints of the 3D bonding pads for each pixel. The PDC can be broken down into four main components, seen in Figure 7.1.

A—Registers and post-processing: registers are used to control the operating modes and the calibration parameters. The PDC has a suite of operations it can do on the timestamps before they are sent out of the chip. These operations will be referred to as the on-chip post-processing. There are two post-processing options that were specifically made in this PDC for QKD: "QKD Relative Timestamp" and " QKD Time-Bin", as seen in Figure 7.2. The first outputs the timestamp relative to the end of the gating window. The second attributes a time-bin value to the event and inserts that value to the output. The behavior of these post-processing operations are influenced by the settings of the registers. Registers are automatically placed and routed in the available area on the chip while respecting timing constraints.

B—SPADs: Single-photon avalanche diodes are photodiodes that are reverse biased beyond their breakdown voltage [49, 17, 26]. Because of this high electric field, an incoming single

photon causes an avalanche current, which is detected and stopped by the quenching circuit. As this metastable operation is similar to that of a Geiger counter tube, the SPADs are said to be operated in "Geiger-mode". The PDC has a 65 nm SPAD 8 × 8 array. The SPADs have a circular 20 µm diameter photosensitive area [43]. The total pixel size is 52.5 µm × 52.5 µm with a pitch of 60 µm. The 8 × 8 array totals 489 µm × 492 µm.

C—TDCs and quenching circuits: There is one TDC for every four SPADs (in a 2 × 2 configuration). Each SPAD has a quenching circuit that controls the avalanche process and resets the SPAD to be triggered again. These quenching circuits are located near the TDCs. TDCs are connected to the quenching signals and determine the time of arrival of the photons. The silver-blue squares in this section are the connection pads for eventual 3D bonding, although not used in this prototype.

D—Input/output pads: These are the IO pads for wirebonding the PDC. The ones on the bottom of Figure 7.1 are for control, communication, and voltage supply. The pads on the right are for wirebonding external SPADs.

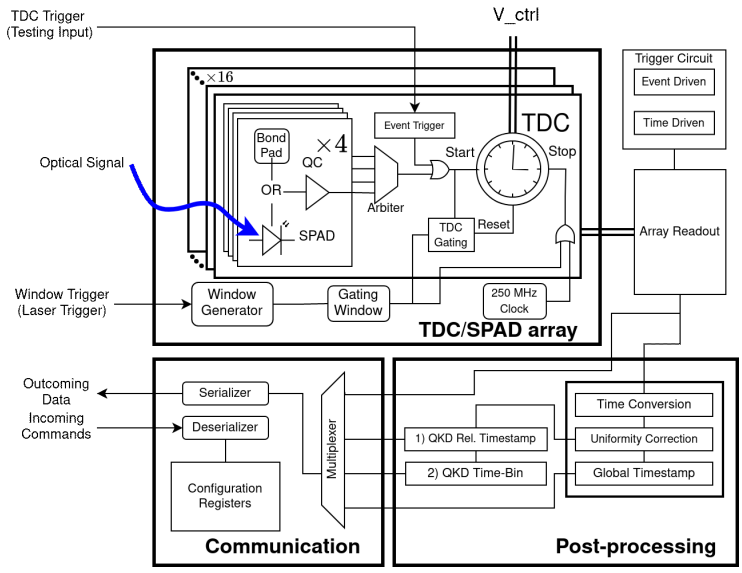

FIGURE 7.2 Block diagram of the all subsystems of the PDC, illustrating the signal flow. Each SPAD of the 8 × 8 array has its own quenching circuit, and 2 × 2 sub-arrays of SPADs are assigned to a TDC (16 in total). The array of TDCs is read out and the data pass through post-processing to the output serializer. The blue arrow indicates an incoming photon on the SPAD.

Figure 7.2 shows how the different elements interact with each other and how the data flows through the PDC.

TDC Gating

The TDC gating circuit (Figure 7.3) determines if an event (QUENCH_*) occurs inside or outside the window of interest in order to remove photon events associated with noise. Because the transmitted photons are sent at a fixed rate, the window is set to be open when they are expected to arrive. Any event that is outside of this window of interest is associated with noise (SPAD noise or ambient light). If outside of the window, it sends a reset signal to the TDC (OUT_WND) so that no timestamp is associated with the event. To keep the jitter of the signal going to the TDC to a minimum, the number of components from the quenching signal (QUENCH_*) to the TDC input is restricted as much as possible. In order to achieve best timing performance, the TDC gating is placed in parallel rather than in line with the SPAD signal. The TDC gating will send a reset signal (OUT_WND) to the TDC if the signal falls outside the gating window. Figure 7.2 shows the TDC gating in a system view where it is connected to the TDCs and gating window.

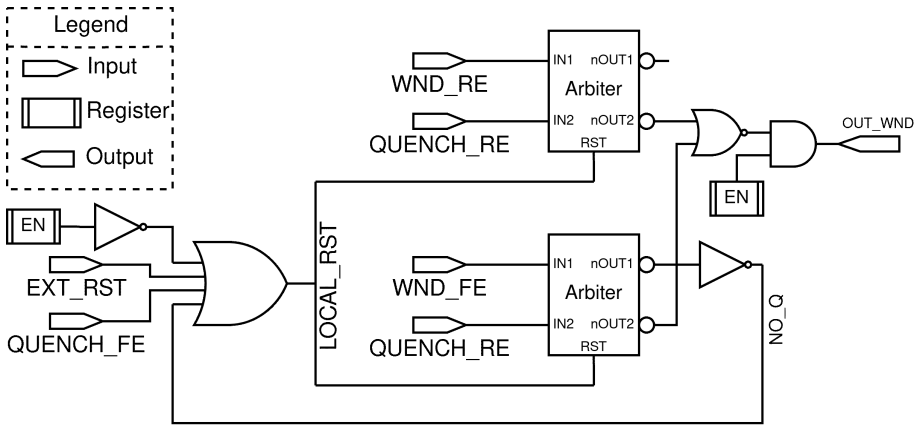

FIGURE 7.3 Simplified schematic of the TDC gating circuit that serves to identify three possible situations: (1) the QUENCH_RE is raised inside the window, (2) the QUENCH_RE is raised before the window, (3) there is no QUENCH_RE inside the window. Cases (1) and (3) are discarded by the circuit keeping OUT_WND low and self-resets. Case (2) causes the OUT_WND signal to raise and the TDC is maintained in a reset state until a next event is permitted. All *_FE (falling edge) and *_RE (rising edge) signals are created with D flip-flops with asynchronous clear.

The most critical component of the TDC gating circuit are the arbiters. They determine which of the two input signals (WND_RE and QUENCH_RE for the top arbiter and WND_FE and QUENCH_RE for the bottom arbiter in Figure 7.3) is raised first. If IN1 is raised before IN2 then nOUT1 goes low (due to active low logic) and nOUT2 remains high. This stays until a reset signal is sent to the arbiter. This can be an external reset of

the system, the end of the event (QUENCH_FE), or an internal reset due to the NO_Q signal.

Data Format and Post-Processing

The data coming out of the chip are packaged in a custom structure and serialized at 250 Mbps. There are multiple data output formats available on the ASIC. The longest one requires 64 bits per TDC, so all data formats were set to this length to simplify data output logic, even if the data volume to be transmitted does not require it.

There are different post-processing modes that can be selected in the chip. The "QKD time-bin" mode uses the TDC gating and on-chip processing to extract which time-bin the event is attributed to. Figure 7.4 illustrates this: first, the timestamp measured by the TDC is made relative to the end of the window. Next, with on-chip programmable boundaries, the timestamps is categorized into one of five time-bins. Bins 1, 2, and 3 are for the three time-bins (LL, EL/LE, and EE) of interest, whereas bins 0 and 4 will contain noise that does not belong to a time-bin in the window. These two extra bins (0 and 4) are to offer more flexibility for assigning time-bins without having to change the window during operation.

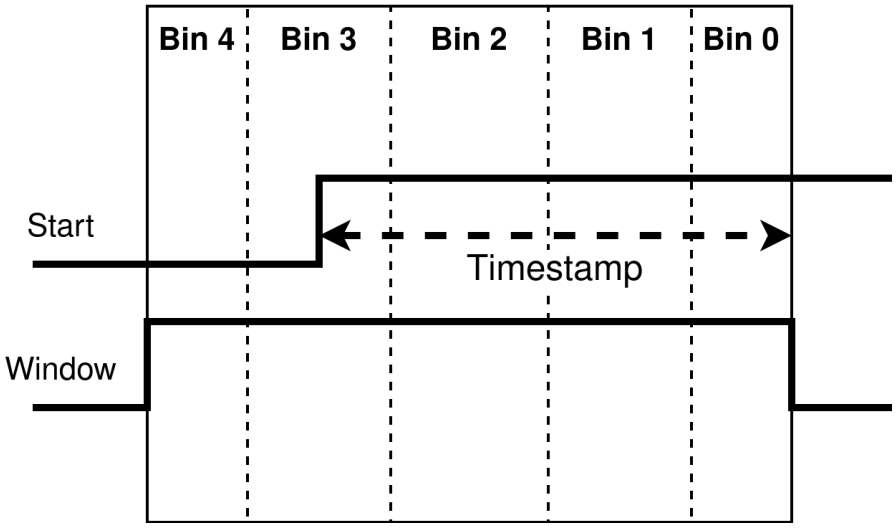

FIGURE 7.4 Using the TDC gating and programmable boundaries, on-chip processing can categorize events into which time-bin they belong. The timestamp is relative to the window instead of the system clock.

Depending on which post-processing is selected, the output data change formats. For example, Figure 7.5 shows the format for the "Time Conversion" post-processing, and Figure 7.6 shows the format for the "QKD Time-Bin" post-processing.

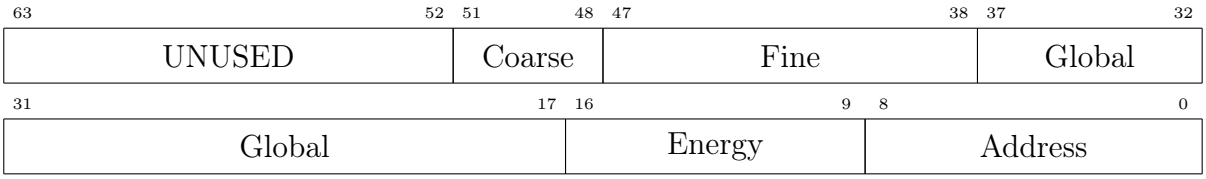

FIGURE 7.5 Dataframe of the the base output mode.
Address [9 bits]: Address of the pixel.
Energy [8 bits]: Number of hits received by that pixel since the last readout.
Global [21 bits]: Timestamp of the system clock (250 MHz).
Fine [10 bits]: TDC fine counter value.
Coarse [4 bits]: TDC coarse counter value.

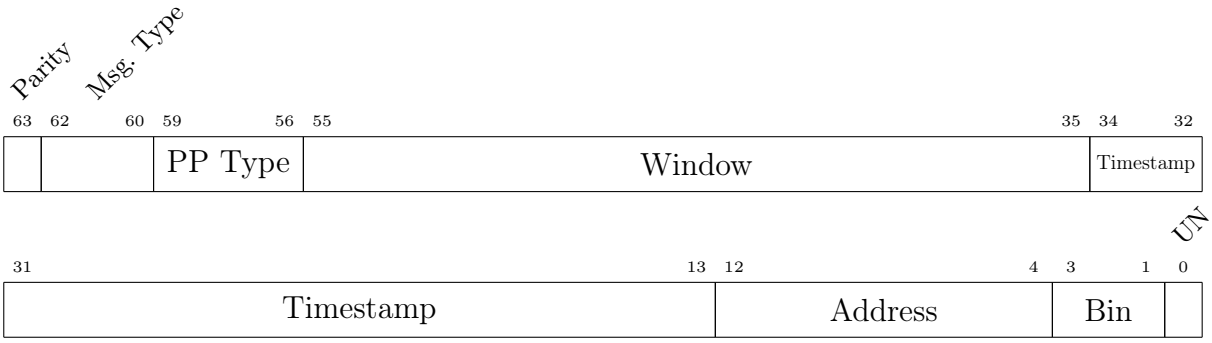

FIGURE 7.6 Dataframe of the the QKD output mode.
UN [1 bit]: Unused.
Bin [3 bits]: In which time-bin value the event is attributed to.
Address [9 bits]: Address of the pixel.
Timestamp [22 bits]: Relative timestamp to the end of the window in picoseconds.
Window [21 bits]: Number of windows since last reset.
PP Type [4 bits]: Post-processing type used. For example, "QKD Rel. Timestamp" or "QKD time-bin". See Figure 7.2.
Msg. Type [3 bits]: Message type. Indicates if it came from array the 8×8 or 1×14 array for example.
Parity [1 bit]: Parity bit check.

Depending on the post-processing selected, the volume of outgoing data can be reduced while retaining the desired information. In Figure 7.6, the most valuable information is the *Bin* and *Window* fields (total 24 bits). The *Bin* field (3 bits) indicates in which time-bin the event was classified. Because the sender and receiver must be synchronized in order to match the sent and received photons, the *Window* field returns the ID of

the window, in other words, if it was the nth window. This would act as a counter to keep the sender and receiver events synchronized, and in a QKD exchange could be as few as 21 bits (26 ms overflow time at 80 MHz rate), as the other fields (40 bits) could be removed (see Figure 7.7). This device therefore helps alleviate the data connection and data processing speed requirements a conventional detector and time-tagging based receiver would encounter for operation of a 64 pixel SPAD array.

To limit afterpulsing (the retriggering of a SPAD due to a lingering charges after an avalanche), the SPAD deadtime is configured to around 80 ns and, due to the set resolution, the approximate TDC deadtime is at most 30 ns. However, as these deadtimes occur in parallel and the internal post-processing is done in pipeline, the PDC's theoretical throughput is limited mainly by the serial data output. As noted previously, the single lane serial link operates at 250 MHz with 64 bit frames. This means that for every event, it takes 256 ns minimum before the data are serialized out of the PDC. Effectively, the serial link imposes a limit on the detection rate of 3.9 MHz. If only the 24 bits in QKD were used, this would increase the upper bound to 10.4 MHz (96 ns period), with the proper frame size.

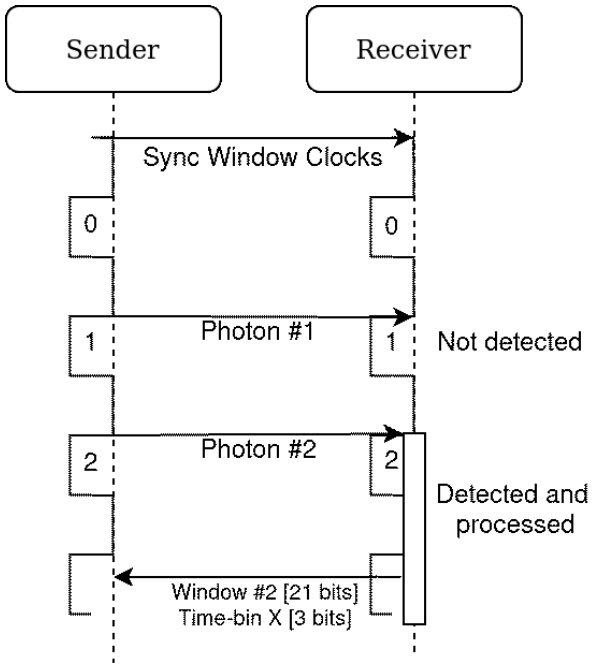

FIGURE 7.7 Diagram of the use of the *Window* field of the dataframe to synchronize the photons sent and received. The initial synchronization of the window clocks could be decided via a sequence of bright pulses or another absolute time reference. This synchronization of the window clock needs be done periodically to compensate for drifting.

7.2.2 Methods and Testing Setups

Testing Setup Structure

The testing setup is divided into three subsystems: the ZCU102, the adapter board, and the head board, as seen in Figure 7.8. The ZCU102 is a commercial board with a ZYNQ FPGA [64]. The adapter board was designed and assembled in-house with all the circuits needed for timing tests (clock generators, delays, buffers, etc.). The PDC is wirebonded on the head board and contains the buffers and voltage regulators.

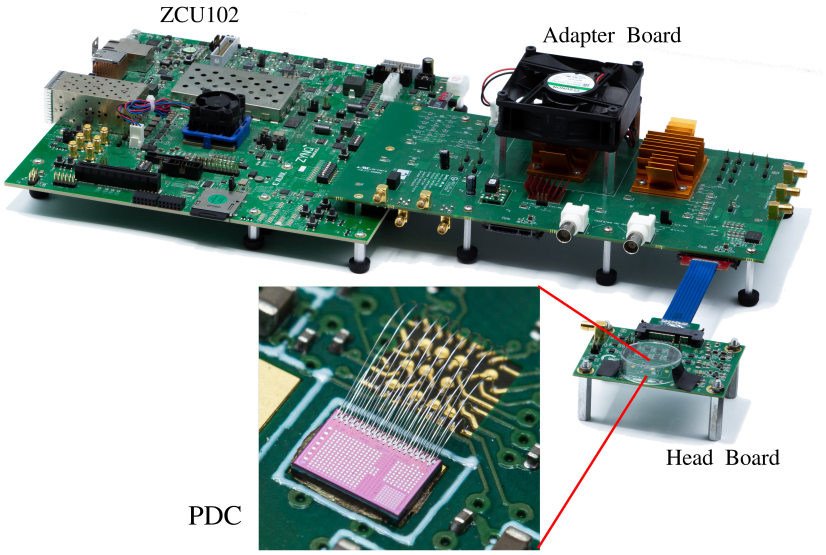

FIGURE 7.8 The complete electronic setup. The adapter board and head boards are connected via a SAMTEC cable to give flexibility to mount the head board within an optical setup. The ZCU102 and adapter boards are connected via a FMC connector to interface the critical signals with the FPGA. The PDC is wirebonded to the head PCB (zoomed view, bottom middle).

There are three main time-sensitive signals that are fed into the PDC: the event trigger, the window trigger, and the 250 MHz clock. Because any jitter on these signals adds jitter to the final result, these signals have to be generated with as little jitter as possible on the printed circuit boards (PCB). The event trigger acts as the start trigger for the TDCs and is routed via an H-tree to all TDCs. It is possible to program the PDC to enable or disable each TDC individually with the registers. The window trigger acts as the start signal for the gating window that is generated on-chip and is also routed in an H-tree. If enabled, the TDCs ignore all events that occur outside of this gating window. The window length can be programmed from 200 to 7500 ps. Finally, the 250 MHz clock acts as the system clock and is the the default “stop” signal of the TDC. That is, by default, timestamps are relative to the system clock of the chip. This can be changed via PDC configuration to

use the end of the gating window as the stop signal. In this case, the timestamps become relative to the end of the gating window.

Optical Tests Setup

The optical test bench uses an ultrafast MaiTai Laser operating at 820 nm that feeds an optical parametric oscillator (OPO) that produces a beam at 410 nm by means of second-harmonic generation. The laser pulse width is <100 fs at an 80 MHz repetition rate (±1 MHz) [37]. The 410 nm beam is directed towards the PDC detector. In order to reduce the laser intensity to be a single photon, neutral density filters are added before reaching the PDC. The 820 nm beam is sent into a low jitter photodiode. The electric pulse generated by this photodiode acts as the time reference and is sent to the PDC.

In typical operation, to get an absolute timestamp, the stop signal of the TDCs is the system clock. However, because we want a timestamp relative to the laser pulse emission for the time-correlated optical tests, the stop signal is programmed to be the end of the gating window. Hence, the output timestamp is the time difference between the arrival of the photon and the end of the window. If TDC gating is enabled, the TDC will ignore all events outside of this window. The window trigger signal can be the output signal of a laser, or, typically, the signal of a low-jitter photodiode as shown in Figure 7.9. The adapter board allows for a variable delay to shift the start of the window until a laser pulse arrives within the window.

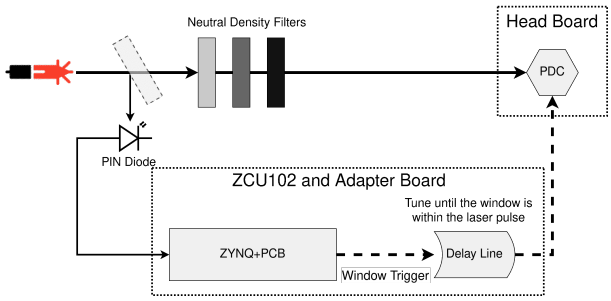

FIGURE 7.9 The setup used for the optical tests. The delay between the PCB and the head board of the window trigger signal is controlled on the board via the ZYNQ and Python scripts. The objective is to match the optical with this electronic delay so that the window trigger starts slightly before the arrival of the beam.

In order to validate the on-chip time-bin QKD functionalities, the optical setup comprises a Mach–Zehnder interferometer (MZI). Figure 7.10 presents a schematic view of the MZI used in the test. As discussed previously, in time-bin QKD, there is a MZI at both the sender and receiver and they must be as identical as possible. To achieve this in a simplified

setup, a mirror (M5) is used to send the photons back through the same MZI to reach a detector placed at the input. Mirror M3 and M4 are mounted on a translation stage (50 mm range) to adjust the path length of the second arm and thus the time difference between the bins. Figure 7.11 shows the full setup with the MZI and detector installed.

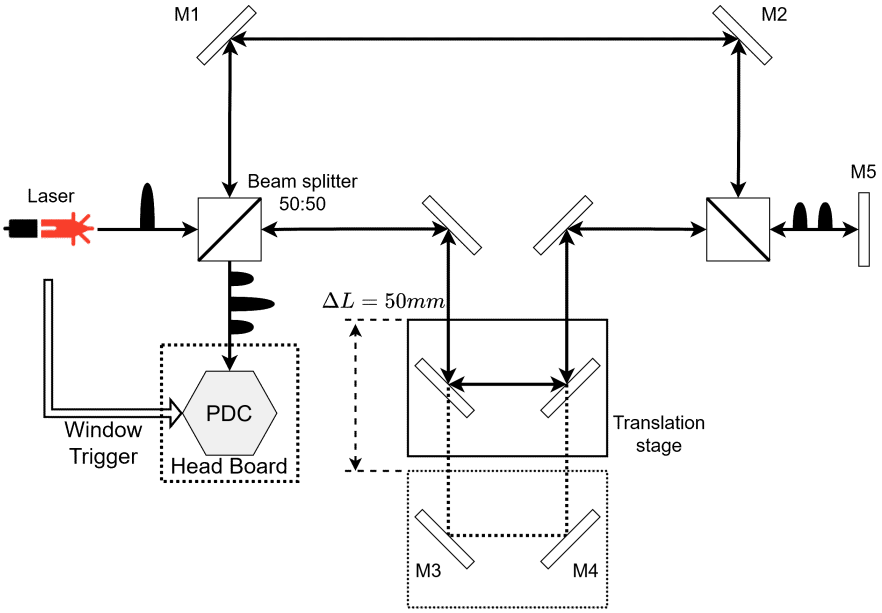

FIGURE 7.10 Basic MZI with a translation stage to control the time-bin separation. A mirror (M5) at the end makes the beam travel the MZI twice to mimic a full sender–receiver path.

Data Acquisition

The data acquisition chain was tailored for the custom PDC, from wirebonding, PCB design, FPGA interfacing, and finally data processing on a computer in Python (see Figure 7.12). In particular, the PCB was designed specifically to minimize the jitter, aiming for less than 10 ps RMS.

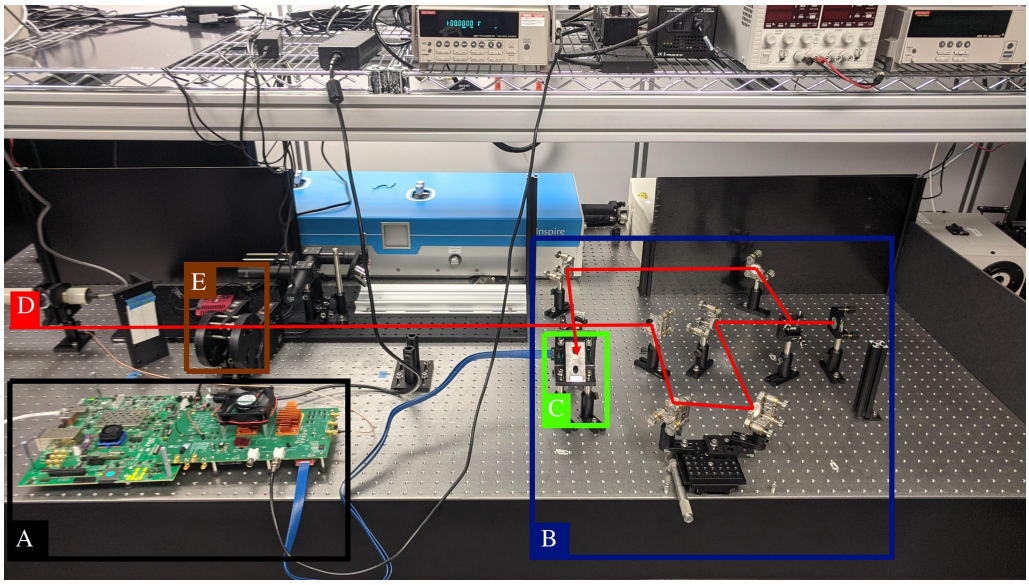

FIGURE 7.11 Laboratory setup for the Mach–Zehnder interferometer. The femtosecond laser comes in from the left (**D**, red). On the left, there is also the control board (**A**, black) for the detector from Figure 7.8. On the right is the MZI optical setup (**B**, blue) with the detector (**C**, green) in the middle, facing back. The optical setup (**B**, blue) is the same as the schematic of Figure 7.10. The neutral density filters (**E**, brown) can adjust laser power.

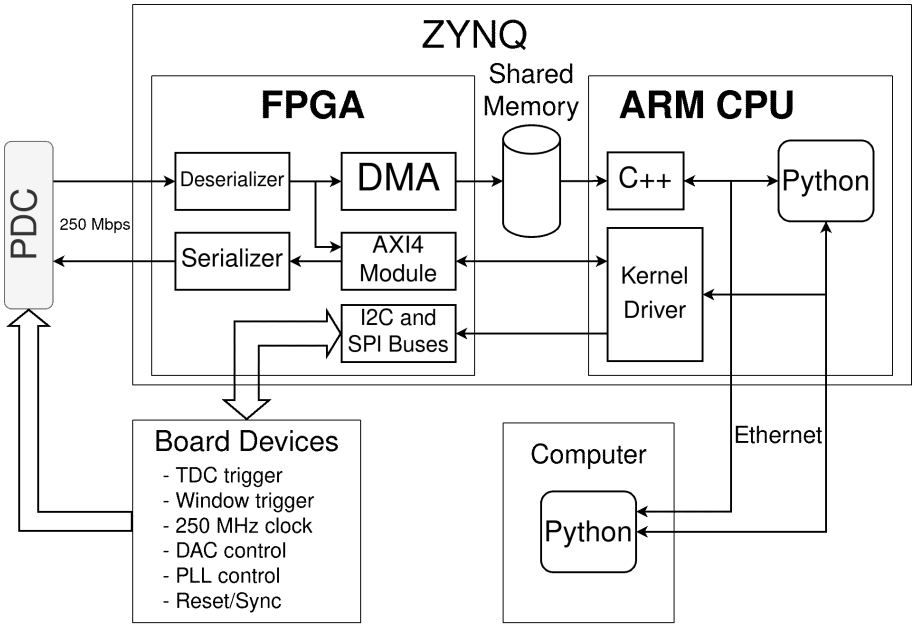

FIGURE 7.12 Simplified dataflow diagram for the data acquisition system. The direct memory access (DMA) allows one to send the data directly to memory space for the CPU to process. Python scripts then record, process, or control the PDC via the kernel driver. As the ARM CPU has access to all resources of the boards, the Python scripts automate most tests.

7.3 Results

This results section is divided into two main sections (electronic and optical) and presents the cumulative jitter from TDCs to time-bin optical measurements. This is to illustrate how the array integration and component design choices impacted the final time-bin measurements. The electronics section presents the results using only the trigger signals from the testing boards presented in Section 7.2.2. The optical section presents the time-bin results done with the setup presented in Section 7.2.2.

7.3.1 Electronic TDC Performance

The TDC architecture used is similar to previous work. More details on the timestamping conversion from TDC raw data can be found in [44, 53].

As an example, Figure 7.13 shows for TDC #0 (head #7) a jitter of 7.48 ps RMS when measured using the system clock as stop signal and a correlated trigger signal generated on the adapter board with a time-delay between these two signals swept from 0 to 4000 ps with steps of 1 ps. We can define the total jitter of the TDC system as Equation (7.1). Because the start and stop signals are correlated, it is not possible to separate the contributions of the start and stop jitter. This is why both are considered together and the measured jitter was <4.2 ps RMS (start is an external trigger and stop is the system clock). This means that the jitter of the TDC can be calculated to be ∼6.2 ps RMS. However, because in a real setting, the jitter of the system ($\text{jitter}_{external}$) does impact the total performance (jitter_{total}), the total jitter will be used in results and comparisons. The jitter breakdown of Equations (7.1)–(7.3) is to understand which components have the most impact and if there are any bottlenecks. Note that in Equations (7.1)–(7.3), $\text{jitter}^2_{\text{external}}$, $\text{jitter}^2_{\text{start and stop}}$, and $\text{jitter}^2_{\text{external trigger and clock}}$ are all the same. *External* is the more generic case, which is essentially the *start and stop* signals, which, in turn, are the *external trigger and clock* in this case.

$$\text{jitter}^2_{\text{total}} = \text{jitter}^2_{\text{TDC}} + \text{jitter}^2_{\text{external}} \tag{7.1}$$

$$= \text{jitter}^2_{\text{TDC}} + \text{jitter}^2_{\text{start and stop}} \tag{7.2}$$

$$= \text{jitter}^2_{\text{TDC}} + \text{jitter}^2_{\text{external trigger and clock}} \tag{7.3}$$

Thus, from jitter_{total} measured at 7.48 ps and $\text{jitter}_{external\ trigger\ and\ clock}$ measured at 4.2 ps, this gives a jitter_{TDC} of ∼6.2 ps. Using the window's end as the stop signal adds jitter to the measurement, as shown in Figure 7.14. In fact, the measured $\text{jitter}_{external}$ changes to <5.2 ps since the stop signal is now the window signal.

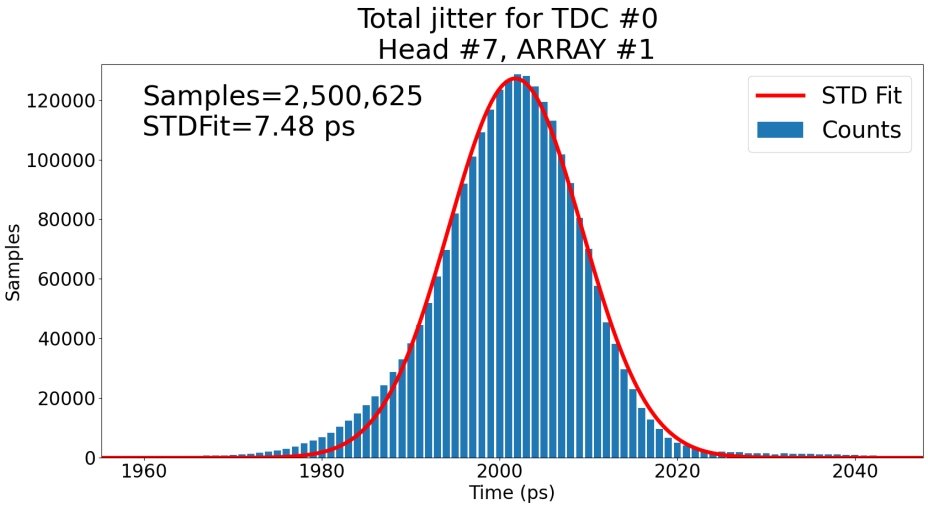

FIGURE 7.13 Total jitter of the TDC #0 of head #7 with all TDCs active for all codes. Sweep the clock-correlated start signal from 0 to 4000 ps with 1 ps steps, centered and aligned at 2000 ps. This result is the sum of all 4001 time delays and aligned. Even though the distribution is not purely Gaussian, the red line is a Gaussian fit to the whole distribution to obtain an estimate of 7.48 ps RMS for the jitter.

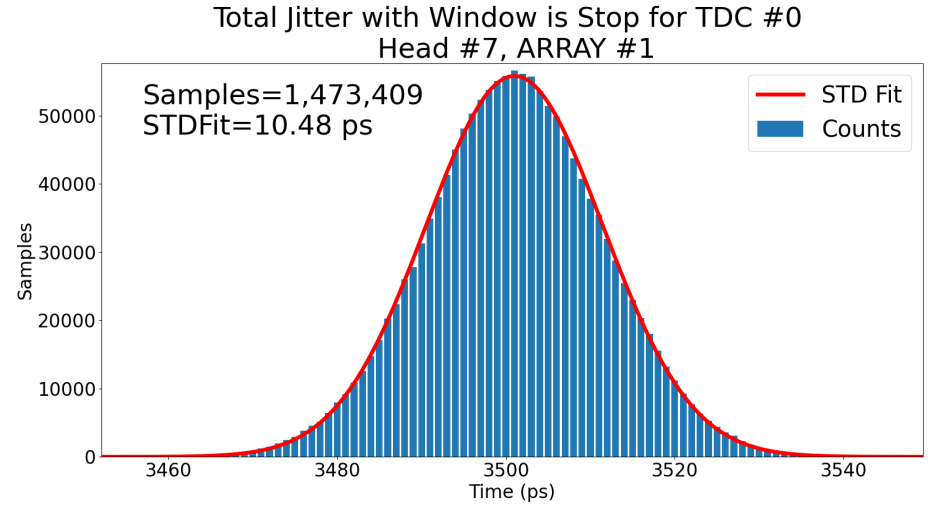

FIGURE 7.14 Total jitter of the TDC #0 of head #7 with all TDCs active with the window as the stop signal. The red line is a Gaussian fit to the whole distribution to obtain an estimate of 10.48 ps RMS for the jitter.

The total jitter is a sum of the contributions of the TDC, the start trigger, and the stop trigger. Equation (7.2) now can be changed as follows:

$$\text{jitter}^2_{\text{total}} = \text{jitter}^2_{\text{TDC}} + \text{jitter}^2_{\text{window circuit}} + \text{jitter}^2_{\text{ext. start trigger and ext. stop trigger}} \tag{7.4}$$

Thus, from jitter_{total} measured at 10.48 ps and $\text{jitter}_{ext.\ start\ trig.\ and\ ext.\ stop\ trig.}$ measured at 5.2 ps, this gives a $\text{jitter}_{TDC} + \text{jitter}_{window\ circuit}$ of ∼9.1 ps. The difference in performance for jitter_{TDC} between Figures 7.13 and 7.14 corresponds to 6.2 ps and 9.1 ps, respectively. This indicates that the window circuit on-chip adds roughly $\sqrt{9.1^2 - 6.2^2} = 6.7$ ps RMS to the jitter. As 6.2 ps and 6.7 ps are so close, the jitter is essentially quadratically doubled when using the window circuit.

Figure 7.15 illustrates the performance uniformity of the TDC array. Although much care was taken to make the TDCs identical and the arrays as uniform as possible, variations in the fabrication process, temperature fluctuations, circuit mismatch, and voltage fluctuations will influence the performance between TDCs. The resolution of the TDCs are tuned with a digital-to-analog converter (DAC). However, as each TDC is slightly different, and the applied voltage is the same for every TDC, some performance variations will occur. The average jitter is 8.4 ps RMS with a 2 ps standard deviation.

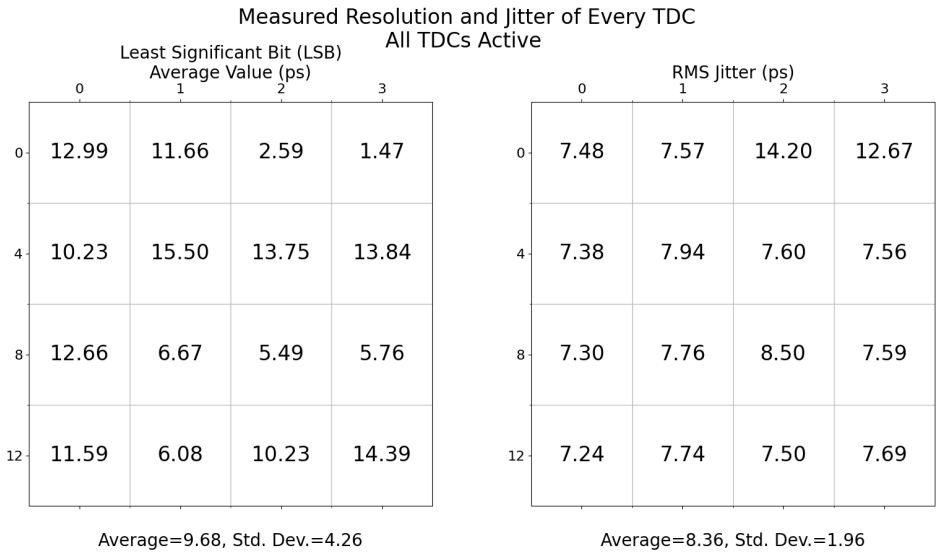

FIGURE 7.15 The resolution (LSB) and jitter of each TDC when all are operating at the same time. These results are for head #7 and array #1 of the chip. Due to variations in the fabrication process, not all TDCs have the exact same performance. This can be seen with the outliers, TDCs 2 and 3, having very fine resolutions and, consequently, higher jitter. The TDCs are indexed from the top left (0) to the bottom right (15), with the index of the leftmost indicated for each row.

7.3.2 Time-Bin Measurements

We now report on the operation of the PDC in the "QKD Time-bin" mode using the setup of Figure 7.10. The following results are from the optical tests in which the three time-bins are measured with the MZI shown in Figure 7.10 at 410 nm wavelength.

In Figure 7.16, the three time-bins (late–late, early–late/late–early, and early–early) are categorized on-chip. They correspond to bins 1, 2, and 3 respectively. Because a late event gets a smaller timestamp measured with respect to the end of the gating window, late–late corresponds to bin 1 (refer to Figure 7.4). Bins 0 and 4 correspond to events that are outside the bounds and are filled with noise triggered events. The bounds between each bins are programmable on-chip. This processing reduces the timestamp information (22 bits) to bin value (3 bits), which maximizes the potential throughput.

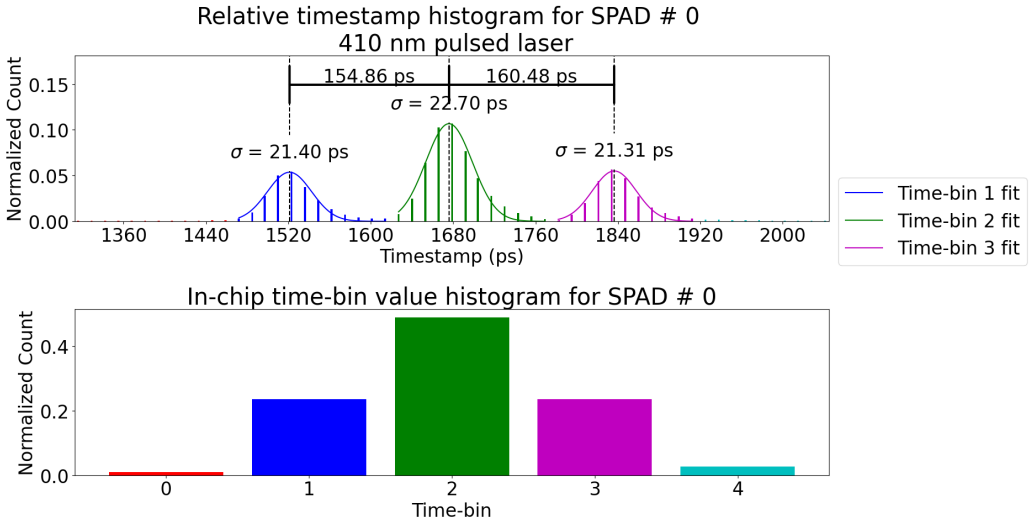

FIGURE 7.16 Time-bin histogram with on-chip timestamping and time-bin categorization. In this case, light was focused on SPAD #0 (connected to TDC #0) to compare the jitter with the previous results. The jitter increases from 10.48 ps to 22.7 ps RMS because the detection chain now includes the SPADs. Each event was categorized into a time-bin (0 to 4), which have programmable boundaries. The bottom histogram shows how many events were categorized in each bin, and the colors match bins between both graphs. Both histograms present the same information, either as relative time of detection or as on-chip categorized time-bins. Because the timestamps are relative to the end of the gating window, the late–late bin is #1, and the early–early is #3. The window size was set to 2.5 ns wide. The histograms are normalized so the total sum is 1.0.

7.3.3 Jitter Estimation for the SPAD and Quenching Circuit Chain

For all time-bin measurements, the start signal of the TDC was the photon arrival and the stop signal was the end of the window signal. The window trigger signal is generated either from another photodiode or from a signal from the laser. Thus, the jitter equation from Equation (7.2) changes to:

$$\text{jitter}^2_{\text{total}} = \left[\text{jitter}^2_{\text{TDC}} + \text{jitter}^2_{\text{window}}\right] + \left[\text{jitter}^2_{\text{SPAD+QC}} + \text{jitter}^2_{\text{laser reference photodiode}}\right] \quad (7.5)$$

$$22.7^2 = 10.48^2 + \left[20.1^2 + 1^2\right] \quad (7.6)$$

The $jitter_{\text{laser reference photodiode}}$ was measured to be 3 ps FWHM with the same setup (laser, photodiode, and oscilloscope) as [43], thus the jitter of the reference photodiode is approximated to <1 ps RMS. From the electrical tests, the jitter of the TDC + window is 10.48 ps RMS when including the jitter of the setup. Therefore, given the $jitter_{total}$ = 22.7 ps RMS from Figure 7.16, that leaves a jitter of ~20.1 ps RMS for the SPAD + quenching circuit (Equation (7.6)).

This is significantly higher than the 7.8 ps FWHM of our previous publication [43]. There are four factors that could explain this difference: (1) this PDC has an array of SPADs instead of a single SPAD channel, (2) the end of the generated window is used as the TDC stop signal, (3) low power 65 nm CMOS (LP) is used instead of general purpose 65 nm CMOS (GP), or (4) design changes to the SPAD layout.

In this PDC, there are 64 SPADs that trigger at an average rate of 680 kcps that generate electrical crosstalk and noise into the power rails or the substrate. Each TDC has two ring oscillators that also generate common-mode noise. In turn, this noise couples to the TDCs and increases their jitter. Jitter measurements were taken while one SPAD channel was activated (others disabled) to compare to when all SPAD channels are active. The jitter did degrade by 1–2 ps RMS in the latter case. Although this does not explain the large difference, it is a contributing factor.

During experiments, it was noticed that some TDC timestamp values would suffer from more jitter when using the window as the stop signal. Although Figure 7.14 shows the impact across all codes, the window might negatively impact certain timestamps that would affect measurements such as those in Figure 7.16, which do not average the jitter across the whole dynamic range.

Due to a higher threshold and less leakage, LP offers lower power consumption at the expense of speed. Although measures were taken to account for these differences, the

impact of the slower speed (compared to GP) might have been bigger than anticipated through simulation.

In this PDC, the quenching circuits read the cathode of each SPAD (as opposed to the anode in [43]). Although the SPAD's architecture was not modified significantly with respect to [43], the connection to the cathode of the SPAD changes the parasitic capacitance at the quenching circuit readout node. For example, one could expect the cathode-to-substrate capacitance to be higher than that of the anode. Such changes would certainly degrade the jitter of the SPAD + quenching circuit.

Because in this PDC we do not have access to the window end signal or the SPAD cathode, it is difficult to give a definitive answer on the source of the added jitter of the SPADs. Although this is still under investigation, the next revision of the PDC will include new unitary test structures in the hope of clearly identifying the cause.

7.4 Discussion

The performances of the TDC array are an improvement over previous iterations [44] from our team and offers additional functionalities such as TDC gating. In [44], TDC jitter performance degradation had been observed when many TDCs were operating simultaneously, injecting noise in the substrate and the power rail. To address this, this iteration made three modifications based on the recommendations of [44]. First, to reduce the common-mode noise, in this integrated circuit there is one TDC for four SPADs. Second, to decrease the mismatch between each TDC, in this version the size of the oscillators' transistors were increased. Third, to equally control the oscillators of the TDCs, we implemented the control voltages of the current starved elements from the ring oscillators in a mesh configuration. These changes proved beneficial, as Figure 7.17 shows that even in an array configuration with all elements active, the performance of the jitter and resolution (LSB) variations are improved with respect to [44].

The new window gating functionality, however, adds more jitter to the system. This can be seen when comparing Figure 7.13 with Figure 7.14 where the jitter increases from 7.48 ps RMS to 10.48 ps RMS just by using the window as the stop signal instead of the system clock. Because the measured jitter of the external signals (the "event trigger" and "window trigger") going into the PDC is ∼4 ps RMS, the PDC is nearing the limits set by the test bench. However, as bigger arrays (such as 64×64) are an objective, ways to reduce the jitter and width variations of the gating window will be explored. The window generator is programmed on-chip to add or remove standard cells delay blocks to control the width of the window. As these delay blocks are susceptible to variations due to tempera-

ture and fabrication, the final width of the window can vary. The window size fluctuations and the routing of the window signal could explain the increase jitter from Figures 7.13 and 7.14 and the increased jitter of SPAD+QC compared to the previous publication [43].

The SPAD array heats the device when activated and that heat is not evenly distributed across the device. As seen in Figure 7.1, there is a SPAD array (B) next to the top side of the integrated read out (C). As they are noisy SPADs, good for electronics and functionality testing, they will generate a hot spot above the read out array (C). This impacts thermal noise and mismatch among electronics pixels. In addition, the routing capacitance between each SPAD and quenching circuit is not equal, which has an impact on the signal slope ($I = C \times dV/dt$), which has a direct impact on the timing jitter.

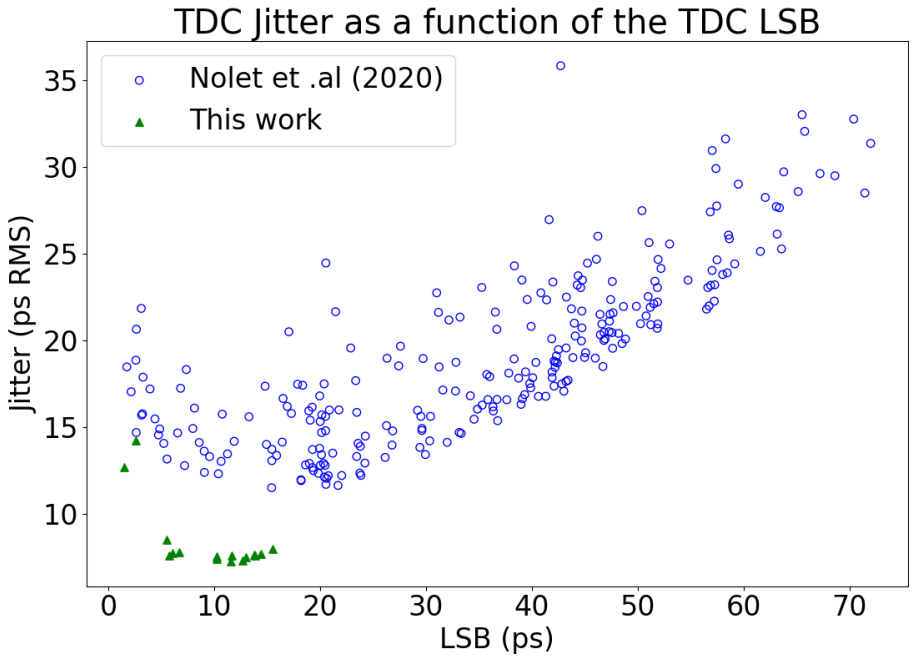

FIGURE 7.17 Jitter as a function of the LSB. The values from Figure 7.15 are compared to the results from Nolet (2020) [44] and illustrate the decreased variation of performance between TDCs. For example, in Nolet (2020), the LSB of every TDC would vary from 2 to 72 ps. In this work, this variation is from 2 to 16 ps.

More investigation is ongoing to understand the extra jitter observed in the measurement and better design techniques. A solution is to use the rising edge of the window instead of the falling edge as the time reference. This could reduce jitter, as the rising edge comes from the signal, compared to the falling edge, which is decided by a series of delay blocks in the window generator.

With the window gating, time-bins with 158 ps difference at 410 nm was achieved. This time difference represents a roughly 5 cm difference between each arm of the MZI and opens doors to explore compact MZI setups. In terms of time-bin separation, this result is similar to other publications [10, 15], but this PDC offers the timestamping done on-chip. This means that no bulky external timestamping equipment is required. These elements, in addition to operating at room temperature, makes this detector a promising candidate for QKD in situations that require small size and low power consumption, such as hand-held or satellite free-space for a QKD network [31, 35].

As noted previously, the SPADs used in this PDC were implemented to provide realistic input to the quenching circuits and TDCs and validate the new QKD functionalities. They are a stopgap solution before the future 3D integrated SPADs that will offer better dark count and photon detection efficiency (PDE). The 65 nm SPADs used in this PDC have a high noise (680 kcps average per SPAD across the 8×8 array) and low PDE (7% at 410 nm). Thankfully, the gating window could be used to reduce their impact. However, the noise restricted how low the laser power could go before losing the signal in the noise floor. This meant that the laser was not operating at a single-photon regime when measuring the time-bins. Because the objective was to demonstrate the functionalities of the PDC and not the security, operating at the single photon level was not an objective of this study but can be implemented in future work. In addition, the measured outgoing event rate coming out of the PDC was around ∼360 KHz (2800 ns period) in the experiment of Figure 7.16. This is much lower than the limit set by the serial communication noted previously (3.9 MHz). We estimate that with the high noise count of the 64 SPAD array, low PDE, and the window gating of 2.5 ns width, the majority of events are rejected by the window gating, and the SPADs are too often in their deadtime. Thus, we are not reaching the upper bound of the event rate.

7.5 Conclusions

The photon-to-digital converter concept allows us to integrate the full detection chain and some signal processing within a single device. In this work, the PDC was designed and implemented as a QKD receiver. The good timing resolution and jitter allows for around 158 ps separation between time-bins while maintaining photon detection rates of several MHz. This translates to more compact MZIs that can be implemented in space-restricted systems and offer easier calibration between the sender and receiver MZI. In addition, TDC gating allows us to reduce noise by only processing events that occur within the window of time the qubit is expected to arrive at the receiver. Finally, custom processing

on-chip (such as on-chip time-binning) offers the possibility to filter unwanted events and extract only the essential data, thus increasing throughput.

These very unique QKD capabilities were demonstrated for this PDC prototype. The 8 $\times$ 8 array of 65 nm SPADs was used to provide realistic input to the system and validate the QKD functionalities of the PDC. Future work includes implementing 3D integrated SPAD design with the PDC to enhance the SPAD performance and adding further on-chip processing capability such as image analysis.

CHAPITRE 8

ATTAQUE PAR CONTRÔLE DE DÉTECTEUR

Aux laboratoires de Waterloo, des attaques DCA (voir sous-section 4.2.4) ont été tentées sur le détecteur. La première étape de l'attaque consiste à aveugler les SPAD du détecteur. La deuxième consiste à faire activer les SPAD en injectant encore plus de lumière pour les maintenir en mode "linéaire". Lors des expériences, la première étape était possible, et certains SPAD devenaient silencieux (aucune sortie). Toutefois, dans tous les essais, jamais la deuxième étape n'a été accomplie. Nous sommes incertains pourquoi ceci est le cas, mais il y a 2 explications possibles: le détecteur est résistant à ce genre d'attaque due à sa configuration de SPAD et circuit d'étouffement, ou les SPAD ne sont pas assez sensibles à la lumière et les faire activer en mode "linéaire" n'est pas possible sans monter la puissance du laser à des niveaux dommageables pour le détecteur. Malheureusement, la réponse à cette question deviendra apparente seulement quand d'autre SPAD à plus faible bruit d'obscurité seront utilisés. La figure 8.1 montre l'image du détecteur avec ses SPAD centraux aveuglés par un laser. Le pixel plus actif (blanc) est fortement illuminé par le laser, mais pas au point d'être aveuglé comme les autres pixels centraux.

Le circuit de détection DCA, quant à lui, réussit à lever l'alerte d'attaque, mais comporte deux failles majeures. La première étant que la valeur maximale du compteur a été choisie trop basse. En effet, durant la conception, l'hypothèse était que le nombre typique de cycles de recharge soit 1 ou 2. Toutefois, ceci n'est pas le cas et le nombre de cycles de recharge peut monter au-delà de 16 (le maximum permis dans la puce) dans une situation extrême. La seconde faille étant que même si le circuit de lecture est mis dans le mode "lire toute la matrice, incluant les TDC qui n'ont pas fait feu", la valeur lue du TDC semble être figée. En d'autres mots, comme il n'y pas de nouvel évènement pour le TDC, la trame ne contient pas le bit indiquant l'attaque DCA du SPAD qui l'a détecté. Comme il y a un bit indiquant l'attaque pour chaque SPAD, si le SPAD n'est pas lu, le bit ne serait pas traité. Donc, l'alerte d'attaque aurait pu être levée, mais comme le pixel ne sort rien, il n'est pas possible de le savoir. Dans la prochaine version, il faudrait un circuit indépendant du circuit de lecture de matrice afin d'inclure correctement la détection d'attaque DCA dans la trame de sortie.

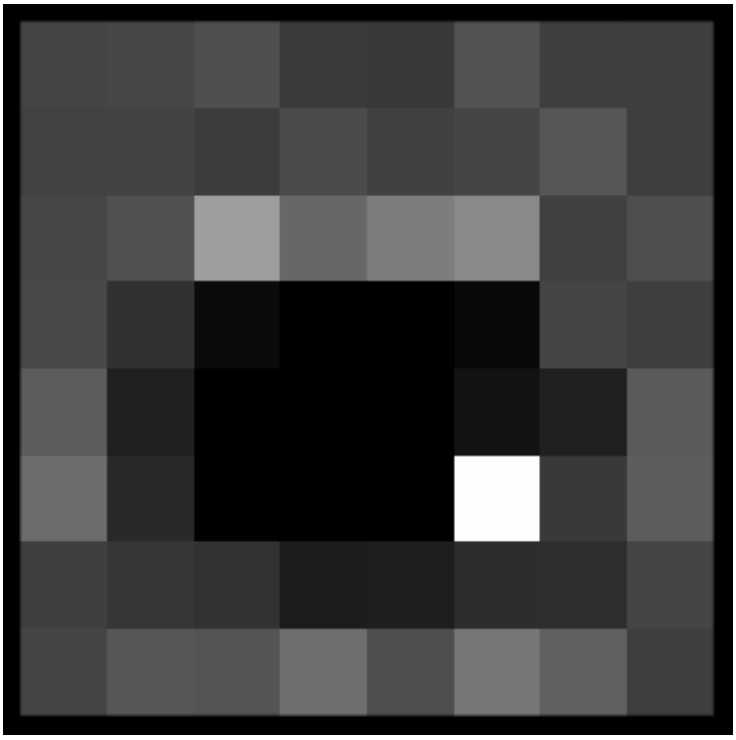

FIGURE 8.1 Image du détecteur avec des SPADs centraux (noir) aveuglés par un laser à 2 mW.

CHAPITRE 9

DISCUSSION

9.1 PLL vs DAC

Il est possible de contrôler la performance des TDC avec les PLL ou les DACs. Dans le cas des expériences QKD, comme les résultats avec PLL avaient plus de gigue temporelle que ceux avec DAC, ce sont les DAC qui sont toujours utilisés. La différence de performance peut être vue à la figure 6.1. Si le lecteur désire plus d'information concernant les performances avec PLL, il peut se référer aux travaux de Michel Labrecque-Dias. Pour voir les performances des TDC en matrice par rapport aux publications précédentes, référez-vous à la section 7.4.

9.2 Les performances du fenêtrage TDC

Le fenêtrage TDC (TDC gating) a été un succès pour les mesures d'encodage temporel QKD. Toutefois, dans les résultats, la gigue temporelle semble être doublée quand la fenêtre est utilisée pour le signal d'arrêt pour le TDC. Pour plus de détails concernant le fenêtrage de TDC et des suggestions d'amélioration, referez-vous à la section 7.4 et sous-section 7.3.1.

9.3 Fonctionnalités pour l'encodage temporel QKD

Comme dit précédemment, des fonctionnalités ont été ajoutées à *ICYSHSR1* pour pouvoir extraire les informations directement avec l'encodage temporel QKD. Des mesures ont été prises en laboratoire avec un interféromètre Mach-Zehnder (MZI) à Sherbrooke et à Waterloo. Ainsi, des mesures de QKD par encodage temporel aux deux laboratoires ont été démontrées et elles présentent les avantages de implémentation choisie. Pour plus de détails concernant les résultats de l'encodage temporel QKD et une discussion sur ces résultats, referez-vous à la sous-section 7.3.2 et à la section 7.4 respectivement.

CHAPITRE 10

CONCLUSION

L'étendue des travaux est grande: de la conception de circuits intégrés, à l'assemblage de PCB et la validation de performances. La question originale revient: quelle est l'implémentation microélectronique d'un circuit permettant la réception de qubits photoniques encodée temporellement ? Au cours de ces travaux, un PDC a été conçu et développé avec l'application de QKD pour but. En utilisant l'encodage temporel, les PDC ouvrent des avenues intéressantes. La plus proéminente étant l'intervalle de temps réduit entre les valeurs de l'encodage temporel. Ceci permet de faire des systèmes plus précis, plus compacts et un encodage plus robuste. La puce produite avait de nouvelles fonctionnalités pour valider le fonctionnement pour le QKD en utilisant l'encodage temporel. Cet objectif a été atteint avec une séparation entre les valeurs d'encodage temporel d'environ 155-160 ps. Cette précision est légèrement plus grande qu'originalement voulu, mais cela reste un résultat très impressionnant dans la littérature.

Cette première itération de la puce a su démontrer 3 fonctionnalités importantes pour le QKD et pour les prochaines versions que j'ai contribuées: fenêtrage TDC, le traitement de signal pour l'encodage temporel et la matrice de SPAD. Le fenêtrage TDC a permis de réduire le bruit en éliminant les évènements qui arrivent à l'extérieur de la fenêtre d'intérêt. De plus, en utilisant la fin de la fenêtre comme référence de temps (contrairement à l'horloge du système), le TDC retourne directement l'étampe temporelle d'intérêt. Grâce à ceci, le traitement de signal ajouté à la puce a pu ensuite calculer la valeur d'encodage temporel avec des limites programmables dans la puce. Le système conçu est entièrement contrôlable via la plateforme de test et le FPGA. J'ai contribué à la majorité du code de contrôle. Grâce à ce code, c'est possible d'automatiser les prises de mesure et même d'avoir une interface graphique pour les mesures en laboratoire optique.

Il y a plusieurs directions intéressantes pour le futur de ce projet. Le plus attirant étant l'intégration 3D avec des SPAD optimisés. C'est l'option qui élèverait le prototype au-delà des autres systèmes QKD utilisés dans le domaine. Comme discuté dans la section 6.2, le décalage interpixel est un problème dont nous ne connaissons pas vraiment la solution. Nous proposons que la variation de décalage entre chaque mesure puisse avoir un lien avec la température du système. Toutefois, dû à l'étendue et au temps limité de ce projet, cette question n'a pas pu être investiguée autant que souhaité. Des travaux futurs pourront

explorer cette question. C'est une situation similaire pour le DCA présentée au chapitre 8. Les résultats semblent nous montrer que le circuit de base est résistant à ce type d'attaque. Or, c'est possible que la basse sensibilité de nos SPAD soit responsable de cette résistance à l'attaque. Plus de travaux devront être faits une fois que des SPAD plus sensibles seront implémentés.

Finalement, comme la turbulence atmosphérique est un problème important pour le QKD dans l'air libre, certains dans la communauté proposent l'utilisation de l'optique adaptative (OA). Cette technique permet de mesurer la distorsion que l'atmosphère apporte à la lumière. La prochaine itération du receveur QKD pourrait inclure des fonctionnalités de OA pour faire du QKD et corriger la distorsion atmosphérique simultanément.

LISTE DES RÉFÉRENCES

[1] Acín, A. et al. (2018). « The Quantum Technologies Roadmap : A European Community View ». In : *New Journal of Physics* 20.8, p. 080201. ISSN : 1367-2630. DOI : 10.1088/1367-2630/aad1ea.

[2] Anisimova, E. (2018). « Single-Photon Detectors for Long Distance Quantum Communications ». http ://hdl.handle.net/10012/12935 : University of Waterloo.

[3] Bell, J. S. (1964). « On the Einstein-Podolsky-Rosen Paradox ». In : *Physics Physique Fizika* 1, p. 195-200. DOI : 10.1103/PhysicsPhysiqueFizika.1.195.

[4] Bennett, C. H. et Brassard, G. (1989). « Experimental Quantum Cryptography : The Dawn of a New Era for Quantum Cryptography : The Experimental Prototype Is Working] ». In : *SIGACT News* 20.4, p. 78-80. ISSN : 0163-5700. DOI : 10.1145/74074.74087.

[5] Bennett, C. et al. (1995). « Generalized Privacy Amplification ». In : *IEEE Transactions on Information Theory* 41.6, p. 1915-1923. ISSN : 0018-9448, 1557-9654. DOI : 10.1109/18.476316.

[6] Bennett, C. H. (1992). « Quantum Cryptography Using Any Two Nonorthogonal States ». In : *Physical Review Letters* 68.21, p. 3121-3124. DOI : 10.1103/PhysRevLett.68.3121.

[7] Bennett, C. H. et Brassard, G. (2014). « Quantum Cryptography : Public Key Distribution and Coin Tossing ». In : *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84 560, p. 7-11. ISSN : 0304-3975. DOI : 10.1016/j.tcs.2014.05.025.

[8] Beutel, F. et al. (2021). « Detector-Integrated on-Chip QKD Receiver for GHz Clock Rates ». In : *npj Quantum Information* 7.1, p. 1-8. ISSN : 2056-6387. DOI : 10.1038/s41534-021-00373-7.

[9] Bienfang, J. C. et al. (2004). « Quantum Key Distribution with 1.25 Gbps Clock Synchronization ». In : *Optics Express* 12.9, p. 2011-2016. ISSN : 1094-4087. DOI : 10.1364/OPEX.12.002011.

[10] Boaron, A. et al. (2018). « Simple 2.5 GHz Time-Bin Quantum Key Distribution ». In : *Applied Physics Letters* 112.17, p. 171108. ISSN : 0003-6951. DOI : 10.1063/1.5027030.

[11] Bourgoin, J.-P. et al. (2013). « A Comprehensive Design and Performance Analysis of Low Earth Orbit Satellite Quantum Communication ». In : *New Journal of Physics* 15.2, p. 023006. ISSN : 1367-2630. DOI : 10.1088/1367-2630/15/2/023006.

[12] Brassard, G. et al. (2000). « Limitations on Practical Quantum Cryptography ». In : *Physical Review Letters* 85.6, p. 1330-1333. DOI : 10.1103/PhysRevLett.85.1330.

[13] Brendel, J. et al. (1999). « Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication ». In : *Physical Review Letters* 82.12, p. 2594-2597. DOI : 10.1103/PhysRevLett.82.2594.

[14] Buttler, W. T. et al. (1998). « Practical Free-Space Quantum Key Distribution over 1 Km ». In : *Physical Review Letters* 81.15, p. 3283-3286. DOI : 10.1103/PhysRevLett.81.3283.

[15] Cahall, C. et al. (2019). « Multi-Mode Time-delay Interferometer for Free-space Quantum Communication ». arXiv : 1908.00852 [physics, physics:quant-ph].

[16] Chen, L. et al. (2016). *Report on Post-Quantum Cryptography*. NIST IR 8105. National Institute of Standards and Technology, NIST IR 8105. DOI : 10.6028/NIST.IR.8105.

[17] Cova, S. et al. (1996-04-20, 1996). « Avalanche Photodiodes and Quenching Circuits for Single-Photon Detection ». In : *Applied Optics* 35.12, p. 1956-1976. ISSN : 2155-3165. DOI : 10.1364/AO.35.001956.

[18] Diffie, W. et Hellman, M. (1976). « New Directions in Cryptography ». In : *IEEE Transactions on Information Theory* 22.6, p. 644-654. ISSN : 0018-9448, 1557-9654. DOI : 10.1109/TIT.1976.1055638.

[19] Einstein, A., Podolsky, B. et Rosen, N. (1935). « Can Quantum-Mechanical Description of Physical Reality Be Considered Complete ? » In : *Physical Review* 47.10, p. 777-780. DOI : 10.1103/PhysRev.47.777.

[20] Ekert, A. K. (1991). « Quantum Cryptography Based on Bell's Theorem ». In : *Physical Review Letters* 67.6, p. 661-663. DOI : 10.1103/PhysRevLett.67.661.

[21] Feynman, R. P. (1982). « Simulating Physics with Computers ». In : *International Journal of Theoretical Physics* 21.6, p. 467-488. ISSN : 1572-9575. DOI : 10.1007/BF02650179.

[22] Gendron, P. (2022). « Amélioration du débit d'évènements, de la qualité des données et de la puissance consommée d'un circuit intégré de photodiodes avalanches monophotoniques ». https ://savoirs.usherbrooke.ca/handle/11143/19204 : Université de Sherbrooke.

[23] Gibson, G. et al. (2004). « Free-Space Information Transfer Using Light Beams Carrying Orbital Angular Momentum ». In : *Optics Express* 12.22, p. 5448-5456. ISSN : 1094-4087. DOI : 10.1364/OPEX.12.005448.

[24] Gisin, N. et Pellaux, J. P. (1992). « Polarization Mode Dispersion : Time versus Frequency Domains ». In : *Optics Communications* 89.2, p. 316-323. ISSN : 0030-4018. DOI : 10.1016/0030-4018(92)90178-T.

[25] Gisin, N. et al. (2002). « Quantum Cryptography ». In : *Reviews of Modern Physics* 74.1, p. 145-195. DOI : 10.1103/RevModPhys.74.145.

[26] Giudice, A. et al. (2007-01-20, 2007). « High-Rate Photon Counting and Picosecond Timing with Silicon-SPAD Based Compact Detector Modules ». In : *Journal of Modern Optics* 54.2-3, p. 225-237. ISSN : 0950-0340. DOI : 10.1080/09500340600763698.

[27] Grover, L. K. (1997). « Quantum Mechanics Helps in Searching for a Needle in a Haystack ». In : *Physical Review Letters* 79.2, p. 325-328. DOI : 10.1103/PhysRevLett.79.325.

[28] Hadfield, R. H. (2009). « Single-Photon Detectors for Optical Quantum Information Applications ». In : *Nature Photonics* 3.12, p. 696-705. ISSN : 1749-4893. DOI : 10.1038/nphoton.2009.230.

[29] Höhn, D. H. (1969). « Depolarization of a Laser Beam at 6328 Å Due to Atmospheric Transmission ». In : *Applied Optics* 8.2, p. 367-369. ISSN : 2155-3165. DOI : 10.1364/AO.8.000367.

[30] Hwang, W.-Y. (2003). « Quantum Key Distribution with High Loss : Toward Global Secure Communication ». In : *Physical Review Letters* 91.5, p. 057901. ISSN : 0031-9007. DOI : 10.1103/PhysRevLett.91.057901. pmid : 12906634.

[31] Jennewein, T. (2018). « Towards Quantum Communications with Satellites ». In : *2018 IEEE Photonics Society Summer Topical Meeting Series (SUM)*, p. 217-218. DOI : 10.1109/PHOSST.2018.8456781.

[32] Jin, J. et al. (2019). « Genuine Time-Bin-Encoded Quantum Key Distribution over a Turbulent Depolarizing Free-Space Channel ». arXiv : 1903.06954 [quant-ph].

[33] Jin, J. et al. (2018-04-19, april 2018). « Demonstration of Analyzers for Multimode Photonic Time-Bin Qubits ». In : *Physical Review A* 97.4, p. 043847. DOI : 10.1103/PhysRevA.97.043847.

[34] Koblitz, N. et Menezes, A. (2016). « A Riddle Wrapped in an Enigma ». In : *IEEE Security and Privacy* 14.6, p. 34-42. ISSN : 1540-7993, 1558-4046. DOI : 10.1109/MSP.2016.120.

[35] Liao, S.-K. et al. (2017). « Satellite-to-Ground Quantum Key Distribution ». In : *Nature* 549.7670, p. 43-47. ISSN : 1476-4687. DOI : 10.1038/nature23655.

[36] Liao, S.-K. et al. (2018). « Satellite-Relayed Intercontinental Quantum Network ». In : *Physical Review Letters* 120.3, p. 030501. DOI : 10.1103/PhysRevLett.120.030501.

[37] *Mai Tai® Ti :Sapphire Ultrafast Laser* (2022). URL : https://www.spectra-physics.com/en/f/mai-tai-ultrafast-laser (visité le 14/09/2022).

[38] Marand, C. et Townsend, P. D. (1995). « Quantum Key Distribution over Distances as Long as 30 Km ». In : *Optics Letters* 20.16, p. 1695-1697. ISSN : 1539-4794. DOI : 10.1364/OL.20.001695.

[39] Marcikic, I. et al. (2002). « Time-Bin Entangled Qubits for Quantum Communication Created by Femtosecond Pulses ». In : *Physical Review A* 66.6, p. 062308. DOI : 10.1103/PhysRevA.66.062308.

[40] Mosca, M. (2016). *Quantum Computing and Cyber-security*. A quantum of prevention for our cybersecurity. URL : https://globalriskinstitute.org/publications/quantum-computing-cybersecurity/ (visité le 16/10/2019).

[41] Moskovich, D. (2015). « An Overview of the State of the Art for Practical Quantum Key Distribution ». arXiv : 1504.05471 [quant-ph].

[42] Nolet, F. (2020). « Électronique d'un convertisseur photon-numérique 3D pour une résolution temporelle de 10 ps FWHM ». http ://hdl.handle.net/11143/17340 : Université de Sherbrooke.

[43] Nolet, F. et al. (2018). « Quenching Circuit and SPAD Integrated in CMOS 65 Nm with 7.8 Ps FWHM Single Photon Timing Resolution ». In : *Instruments* 2.4, p. 19. ISSN : 2410-390X. DOI : 10.3390/instruments2040019.

[44] Nolet, F. et al. (2020). « A 256 Pixelated SPAD Readout ASIC with In-Pixel TDC and Embedded Digital Signal Processing for Uniformity and Skew Correction ». In : *Nuclear Instruments and Methods in Physics Research Section A : Accelerators, Spectrometers, Detectors and Associated Equipment* 949, p. 162891. ISSN : 0168-9002. DOI : 10.1016/j.nima.2019.162891.

[45] *NSA Suite B Cryptography - NSA/CSS* (2015). URL : https://web.archive.org/web/20151123081120/https://www.nsa.gov/ia/programs/suiteb_cryptography/ (visité le 15/10/2019).

[46] Oi, D. K. L. et al. (2017). « Nanosatellites for Quantum Science and Technology ». In : *Contemporary Physics* 58.1, p. 25-52. ISSN : 0010-7514. DOI : 10.1080/00107514.2016.1235150.

[47] Parent, S. (2022). « Design of a Vertically Integrated Single-Photon Avalanche Diodes, Manufactured at Wafer Level, for a Photon-to-Digital Converter Technology ». https://savoirs.usherbrooke.ca/handle/11143/20119 : Université de Sherbrooke.

[48] Planck, M. et Masius, M. ([c1914]). *The Theory of Heat Radiation*. Avec la coll. d'University of California Libraries. Philadelphia, P. Blakiston's Son & Co. 256 p.

[49] Pratte, J.-F. et al. (2021-01, 2021). « 3D Photon-to-Digital Converter for Radiation Instrumentation : Motivation and Future Works ». In : *Sensors* 21.2, p. 598. ISSN : 1424-8220. DOI : 10.3390/s21020598.

[50] Razavi, M. et al. (2019). « Quantum Key Distribution and beyond : Introduction ». In : *JOSA B* 36.3, QKD1-QKD2. ISSN : 1520-8540. DOI : 10.1364/JOSAB.36.00QKD1.

[51] Roberts, G. L. et al. (2017). « Modulator-Free Coherent-One-Way Quantum Key Distribution ». In : *Laser & Photonics Reviews* 11.4, p. 1700067. ISSN : 1863-8899. DOI : 10.1002/lpor.201700067.

[52] Roy, N. (2015). « Réalisation d'un convertisseur temps-numérique en CMOS 65 nm pour une intégration par pixel dans un module de comptage monophotonique ». http ://hdl.handle.net/11143/8142 : Université de Sherbrooke.

[53] Roy, N. et al. (2017). « Low Power and Small Area, 6.9 Ps RMS Time-to-Digital Converter for 3-D Digital SiPM ». In : *IEEE Transactions on Radiation and Plasma Medical Sciences* 1.6, p. 486-494. ISSN : 2469-7303. DOI : 10.1109/TRPMS.2017.2757444.

[54] Sajeed, S. et Jennewein, T. (2021-06-07, 2021). « Observing Quantum Coherence from Photons Scattered in Free-Space ». In : *Light : Science & Applications* 10.1, p. 121. ISSN : 2047-7538. DOI : 10.1038/s41377-021-00565-y.

[55] Scarani, V. et al. (2004). « Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations ». In : *Physical Review Letters* 92.5, p. 057901. ISSN : 0031-9007. DOI : 10.1103/PhysRevLett.92.057901. pmid : 14995344.

[56] Scarani, V. et al. (2009). « The Security of Practical Quantum Key Distribution ». In : *Reviews of Modern Physics* 81.3, p. 1301-1350. DOI : 10.1103/RevModPhys.81.1301.

[57] Schmitt-Manderbach, T. et al. (2007). « Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 Km ». In : *Physical Review Letters* 98.1, p. 010504. DOI : 10.1103/PhysRevLett.98.010504.

[58] Shor, P. (1994). « Algorithms for Quantum Computation : Discrete Logarithms and Factoring ». In : *Proceedings 35th Annual Symposium on Foundations of Computer Science*, p. 124-134. DOI : 10.1109/SFCS.1994.365700.

[59] Shor, P. W. (1997). « Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer ». In : *SIAM Journal on Computing* 26.5, p. 1484-1509. ISSN : 0097-5397. DOI : 10.1137/S0097539795293172.

[60] Shor, P. W. et Preskill, J. (2000). « Simple Proof of Security of the BB84 Quantum Key Distribution Protocol ». In : *Physical Review Letters* 85.2, p. 441-444. DOI : 10.1103/PhysRevLett.85.441.

[61] Sibson, P. et al. (2017-02-20, 2017). « Integrated Silicon Photonics for High-Speed Quantum Key Distribution ». In : *Optica* 4.2, p. 172-177. ISSN : 2334-2536. DOI : 10.1364/OPTICA.4.000172.

[62] Wang, S. et al. (2014). « Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network ». In : *Optics Express* 22.18, p. 21739-21756. ISSN : 1094-4087. DOI : 10.1364/OE.22.021739.

[63] Yin, H.-L. et al. (2016). « Measurement-Device-Independent Quantum Key Distribution Over a 404 Km Optical Fiber ». In : *Physical Review Letters* 117.19, p. 190501. DOI : 10.1103/PhysRevLett.117.190501.

[64] *Zynq UltraScale+ MPSoC ZCU102 Evaluation Kit* (2022). URL : https://www.xilinx.com/products/boards-and-kits/ek-u1-zcu102-g.html (visité le 04/12/2022).