Universidad de Concepción
Dirección de Postgrado
Facultad de Ingeniería - Doctorado en Ciencias de la Ingeniería
con mención en Ingeniería Eléctrica

APLICACIÓN DE ELECTRÓNICA EMBEBIDA DE BAJO COSTO EN EL PROCESAMIENTO DE INFORMACIÓN CUÁNTICA

Tesis para optar al grado académico de
Doctor en Ciencias de la Ingeniería con mención en Ingeniería Eléctrica.

JAIME ANDRES CARIÑE CATRILEO

CONCEPCIÓN-CHILE

2016

Profesor Guía: Dr. Guilherme Barreto Xavier.
Profesor Co-Guía: Dr. Miguel Figueroa Toro.
Dpto. de Ingeniería Eléctrica, Facultad de Ingeniería
Universidad de Concepción.

APLICACIÓN DE ELECTRÓNICA EMBEBIDA DE BAJO COSTO EN EL PROCESAMIENTO DE INFORMACIÓN CUÁNTICA

POR: JAIME ANDRES CARIÑE CATRILEO.

Comisión Examinadora:

Dr. Guilherme Barreto Xavier.
Profesor Guía

Dr. Miguel Figueroa Toro.
Profesor Co-Guía

Dr. Gustavo Lima Moreira.
Profesor Externo

Octubre 2016
Concepción, Chile.

Dedicado a mi mujer María,
y a mis hijas Isabel y Denise.

Agradecimientos

Quiero agradecer a la Comisión Nacional de Ciencia y Tecnología (CONICYT), quienes financiaron completamente mis estudios de doctorado en Chile, además de agradecer al Centro de Óptica y Fotónica (CEFOP) por aportar el equipamiento e instalaciones utilizadas en el desarrollo de este trabajo de tesis. También quiero expresar mi gratitud a mis supervisores G. B. Xavier y M. Figueroa, quienes incondicionalmente me brindaron todo el apoyo académico, ya que sus valiosos aportes y evaluaciones lograron que pudiera terminar con éxito este proyecto. Finalmente, mis infinitos agradecimientos a mi mujer María y mis hijas Isabel y Denise por brindarme todo su apoyo moral y estar a mi lado en esta etapa de mi vida.

Resumen

La criptografía protege la información de un mensaje utilizando una clave. Esta tarea se realiza con técnicas que se basan en el poder computacional actual, para mantener segura la codificación y la distribución de la clave. Sin embargo, los avances en información cuántica permitirán el desarrollo de la computación cuántica, la cual tendrá un dramático poder de computación ante tareas especificas, haciendo vulnerable la utilización y la distribución de clave protegida con técnicas tradicionales.

Por otro lado, la imposibilidad de medir ni clonar estados cuánticos, sin perturbar el sistema, impulsa el desarrollo del área de distribución cuántica de claves (QKD). En QKD es posible distribuir una clave entre dos puntos distantes, asegurando la absoluta privacidad de ésta a través de las propiedades de la mecánica cuántica. Los protocolos QKD pueden desarrollarse con la utilización de estados cuánticos codificados en fotones. Esto ha permitido implementar enlaces cuánticos a través de sistemas de fibras ópticas comerciales. Este tipo de enlace introduce ruido y perturbaciones a las propiedades cuánticas de los fotones, efectos que sumados al ruido electrónico en la generación y detección de estados, aumentan la tasa de error de bits cuánticos (QBER), disminuyendo visibilidad de los estados cuánticos.

Este trabajo muestra la relación proporcional de la visibilidad de estados cuánticos y la resolución electrónica de detección. En base a esto, proponemos que es posible diseñar sistemas electrónicos avanzados en electrónica comercial de bajo costo, para sistemas cuánticos que requieren alta precisión en sincronismo y disminución controlada de ruidos y perturbaciones electrónicas, mejorando parámetros como la visibilidad de estados cuánticos sobre enlaces de larga distancia, los cuales pueden ser utilizados para criptografía utilizando protocolos QKD. En base a esto, logramos establecer enlaces con fotones entrelazados cuánticamente certificados en laboratorio y a $3{,}7km$ de fibra óptica instalada en terreno, uniendo instalaciones dentro de la Universidad de Concepción. Por otro lado, en base a sistemas embebidos habilitamos sistemas QKD de altas dimensiones con enlaces de fibra óptica multicore, y además implementamos un protocolo que permite la generación de números aleatorios privados, el que puede ser más seguro que los generadores convencionales, y por sus características es factible su aplicación en sistemas QKD actuales.

Tabla de contenidos

Dedicatoria **iii**

Agradecimientos **iv**

Resumen **v**

Índice de tablas **ix**

Índice de figuras **x**

Capítulo 1. Introducción **2**

1.1. Criptografía cuántica 2
1.2. Herramientas 4
1.3. Propuesta 5
1.4. Hipótesis 6
1.5. Objetivos 6
1.5.1. Objetivo general 6
1.5.2. Objetivos específicos 6

Capítulo 2. Distribución cuántica de claves para criptografía **9**

2.1. Criptografía 9
2.1.1. Técnicas criptográficas 9
2.1.2. One-time-pad 11
2.2. Formalismo cuántico 11
2.2.1. Quantum bit 11
2.2.2. Sistemas multidimensionales 13
2.2.3. Sistemas compuestos 14
2.2.4. Entrelazamiento 14
2.2.5. Mutually unbiased bases 15

2.3. Distribución cuántica de claves 17
2.3.1. Protocolo BB84 17
2.3.2. QKD en altas dimensiones 19
2.3.3. Protocolo QKD de Artur Ekert 20

Capítulo 3. Desigualdades de Bell **23**
3.1. Medición cuántica del entrelazamiento 23
3.2. Desigualdad de CHSH 25
3.3. Contradicción cuántica evaluando las desigualdad CHSH 28
3.4. Generalización de la desigualdad de CHSH (I-Chained) 28
3.5. Loopholes en la mecánica cuántica 29

Capítulo 4. Sistemas embebidos en comunicación cuántica **32**
4.1. Muestreo digital de alta resolución 33
4.2. Arquitectura Contador de coincidencia 35
4.2.1. Módulo string-to-radius 35
4.2.2. Retraso electrónico para cuentas en coincidencias 37
4.3. Evaluación del diseño desarrollado 38

Capítulo 5. Aumento de visibilidad óptica en configuraciones con entrelazamiento cuántico **44**
5.1. Entrelazamiento energía-tiempo 44
5.2. Control de fase en interferómetro de Mach-Zehnder 48
5.3. Control proporcional integral derivativo 50
5.4. Control de fase en entrelazamiento energía tiempo 51
5.5. Resultados preliminares en entrelazamiento energía tiempo 53
5.6. Caracterización de variación de fase en interferómetro de fibra montado en terreno 55
5.7. Estabilización de fase para interferómetro de fibra instalada en terreno . . . 58
5.8. Evaluación de enlace cuántico instalado en terreno 61
5.9. Resultados experimentales evaluando Chained-Bell-Inequalities 63

Capítulo 6. Generación de números aleatorios privados **67**
6.1. Sistema cuántico para generación de números aleatorios privados 67
6.1.1. Quantum random access code 68
6.1.2. Protocolo para generación de números aleatorios privados 70
6.1.3. Umbral para evaluación de privacidad 70
6.2. Implementación experimental 72
6.3. Resultados obtenidos 74

Capítulo 7. Sistema cuántico de alta dimensión para QKD **77**
7.1. Sistema cuántico de alta dimensión utilizando fibra óptica multicore 77
7.1.1. Generación de ququart 81
7.1.2. Resultados preliminares transmisión de ququart 81

Capítulo 8. Conclusiones **86**
8.1. Conclusión General 86
8.2. Conclusiones Específicas 86

Bibliografía **89**

Apéndice A. Producción **96**

Apéndice B. El qubit **98**

Apéndice C. Los postulados de la mecánica cuántica **101**

Apéndice D. Teorema de non-cloning **104**

Apéndice E. Potencia óptica sobre un interferómetro de Mach-Zehnder **106**

Apéndice F. Potencia óptica sobre interferómetro MZ instalado en terreno **109**

Índice de tablas

4.1. Evaluación del error electrónico y t_w utilizando 500ps. 41
4.2. Estadística del error electrónico de una unidad CCU, para distintas resoluciones t_r. 41

B.1. Estados obtenidos dentro de la esfera de Bloch. 100

Índice de figuras

2.1. Sistema general de comunicación secreta. 10
2.2. Esfera Bloch 12

3.1. Configuración experimental, para explicar el entrelazamiento cuántico. 24

4.1. Diagrama de muestreo digital. 34
4.2. Diagrama Arquitectura Contador con resolución de $500ps$ 36
4.3. Cuentas coincidentes experimentales en una ventana tw. 39
4.4. Fitting experimental utilizando una ventana de detección en coincidencia de $t_w = 3ns$. 40

5.1. Esquema de Franson, para entrelazamiento energía-tiempo 44
5.2. Interferómetro en configuración hug, para entrelazamiento energía-tiempo 46
5.3. MZI como controlador de fase 48
5.4. Medición de potencia experimental (en unidades arbitrarias), de interferómetro MZI armado en mesa óptica. 49
5.5. Diagrama de bloque del sistema modelado. 50
5.6. Configuración experimental para evaluación de entrelazamiento energía tiempo. 52
5.7. Resultados obtenidos del control sobre el sistema montado en el laboratorio. 53
5.8. Detecciones en coincidencias sobre la región simétrica. 54
5.9. Curvas de interferencia y violación de las desigualdades CHSH. . . 55
5.10. Configuración experimental para evaluación de entrelazamiento energía tiempo con fibras instaladas en terreno. 56
5.11. Detección de señal de control sobre el foto-detector p-i-n fibra montada en terreno. 57

5.12. Diagrama de bloques, nuevo modelo de sistema con perturbaciones por brazos. 58
5.13. Diagrama de control con "media móvil" en interferómetro con perturbaciones por brazos. 59
5.14. Estabilización de fase 3.7km de fibra instalada en terreno. 60
5.15. Visibilidad de estados cuánticos sobre enlace de 3.7km. 61
5.16. Resultados experimentales para evaluación de la desigualdad CHSH. 62
5.17. Configuración experimental para evaluación de desigualdad de $I_{chained}$. 63
5.18. Violación experimental de la desigualdad de $I_{chained}$ utilizando $n = 3$. 65

6.1. Escenario de preparación y medida de nuestro protocolo SDI para generación de números aleatorios privados. 68
6.2. Configuración experimental para obtención de números aleatorios privados. 73
6.3. Resultados experimentales evaluados sobre p_{AV}^{umbral}. 74
6.4. Probabilidades teóricas y experimentales obtenidas para una configuración QRAC $2 \rightarrow 1$. 75

7.1. Generación de sistema cuántico con dimensión 4. 78
7.2. Mediciones ópticas sobre la salida en Bob. 79
7.3. Modulación de fase en dimensión 4, para Alice y Bob. 80
7.4. Evaluación de la fidelidad de los estados cuánticos generados por el sistema. 82
7.5. QBER experimental en configuración pasiva. 83
7.6. QBER experimental en configuración utilizando control activo. . . . 84

B.1. El qubit y coordenadas polares. 99
B.2. El qubit y coordenadas polares. 100

E.1. MZI con fase controlada a través de un piezo-eléctrico. 106

F.1. Detección de señal de control sobre el fotodetector p-i-n fibra montada en terreno. 109

CAPÍTULO 1

INTRODUCCIÓN

Capítulo 1

Introducción

La Criptografía se basa en codificar mensajes con una clave (obteniendo un criptograma), de tal forma de que sólo quien conozca la clave pueda tener acceso a la información. Con esto, la seguridad del criptograma dependerá exclusivamente de la privacidad de la clave.

Actualmente, algunos algoritmos criptográficos se basan en el poder computacional para codificar mensajes [1], haciendo que el criptoanálisis realizado por un espía para obtener la información codificada, sea una tarea imposible con el poder computacional actual. Sin embargo, las técnicas criptográficas actuales serán vulnerables ante algoritmos ejecutados con los futuros computadores cuánticos, los cuales brindarán un dramático poder computacional a tareas específicas [2].

Los computadores cuánticos se han estudiado en el área de investigación denominado información cuántica (QI), la cual ha evolucionado rápidamente [3, 4], haciendo que los computadores cuánticos sean una realidad factible, tomando un peligroso rol en la privacidad de las comunicaciones.

1.1. Criptografía cuántica

Por otro lado, no se puede clonar estados cuánticos desconocidos [5], ni realizar mediciones sin perturbar el sistema [6]. Luego, si una persona no autorizada intercepta parte de la información transmitida, las mediciones son perturbadas, generando un error que puede ser detectado estimando la tasa del error del bit cuántico (QBER). Entonces, observando los niveles de QBER y estableciendo un umbral, dos entes podrán compartir información privada, desechando ésta cuando un tercero sea detectado entrometiéndose en el enlace cuántico. Esta propiedad impulsa el desarrollo del área de investigación denominada *Quantum Key Distribution*(QKD), la que permitiría distribuir claves para criptografía en dos puntos distantes, asegurando la privacidad de dicha clave.

Es así como aparecen los protocolos BB84 y el B92 [7, 8]. Estos protocolos pueden ser empleados utilizando estados cuánticos de altas dimensiones, haciendo más compleja la tarea de criptoanálisis, aumentando análogamente la seguridad en QKD. Otra de las ventajas de trabajar con altas dimensiones, es que el sistema permite operar con un QBER más alto, sin perder seguridad en el enlace. Aunque este campo es poco explorado, ya hay resultados que demuestran la factibilidad de la utilización de altas dimensiones [9].

Otra de las particularidades de este tipo de protocolos, es que distribuyen y generan una clave o cadena aleatoria. Esta clave se genera emitiendo y detectando estados aleatoriamente, por esto los protocolos dependen de la utilización de generadores de números aleatorios, tales como generadores cuánticos de números aleatorios (QRNG) [10]. Sin embargo, si un agente externo altera este tipo de generador, de tal forma que las estaciones generen una trama aleatoria, pero conocida por el espía, la clave generada no será privada y los usuarios no podrán detectar la intromisión del espía, ya que este tipo de ataques no altera el QBER.

Otro protocolo es el conocido como Ekert91 [11], el cual no utiliza generadores de números aleatorios, ya que se implementa con la generación espontánea de pares entrelazados. Los pares son separados y enviados a dos puntos distantes entre ellos, si estos están entrelazados, la medición de ambos en tiempos simultáneos arrojará resultados correlacionados entre ellos, permitiendo generar una clave completamente privada en ambos extremos. Para certificar el entrelazamiento entre las partículas se utilizan las desigualdades de Bell [12], cuyo resultado delataría la intromisión de un tercero, completando el protocolo.

Para evaluar las desigualdades de Bell, y por tanto certificar el entrelazamiento, se utilizan las probabilidades obtenidas de las mediciones cuánticas sobre el sistema, si estas superan un umbral, la desigualdad se viola. Una de estas desigualdades es conocida como desigualdad *CHSH* [13], la cual es un resultado particular de la desigualdad de *I-Chained* [14].

El protocolo Ekert91 aún es poco práctico, ya que sólo a fines del 2015 se logra la violación de las desigualdades de Bell sin “loopholes” (circunstancias experimentales que obligaban a tomar supuestos extras para lograr la violación)[15], y utilizando entrelazamiento en la alineación del “Spin” de dos electrones distantes [16].

Las partículas pueden entrelazarse en distintos grados de libertad, entre ellos está el entrelazamiento energía-tiempo [17]. El esquema más utilizado para generar este tipo de entrelazamiento, es un interferómetro de Franson [18]. El problema de este esquema es que tiene un loophole geométrico intrínseco, denominado loophole de post-selección [19]. Para evitar este loophole, Cabello propone un cambio geométrico en base a un interferómetro llamado configuración "Hug" [17], el cual fue implementado en espacio libre y a pocos centímetros de separación [20].

La configuración geométrica anterior, sumado al aumento de distancia de separación entre los usuarios, permitiría la ejecución de protocolos Ekert91 en base a entrelazamiento energía-tiempo. Sin embargo, un enlace en fibra óptica presenta problemas de atenuación, perturbaciones y ruido en las propiedades cuánticas de los estados emitidos, haciendo de suma importancia la utilización de técnicas activas para estabilizar el enlace [21].

1.2. Herramientas

Las mediciones, control y procesamiento de datos para experimentos en información cuántica deben ser en tiempo real y con resolución de trabajo en nano segundos. Por este motivo, una solución digital de bajo costo es el empleo de *field programmable gate array* (FPGA) en el desarrollo de sistemas para QI, tales como sistemas QKD [22, 23, 24], y unidades contadoras de coincidencias (CCU) [25, 26, 27, 28, 29].

Los FPGA son un arreglo de compuertas y recursos digitales, cuya lógica y conexión son completamente configurables, presentando máxima velocidad de información digital entre los dispositivos interconectados, además de permitir cambios sobre el circuito dentro del chip en cualquier momento. Esto, sumado a la utilización de unidades *Intellectual Property* (IP) *core*, integrados en un FPGA [30, 31], han permitido diseños de sistemas QKD sobre FPGAs a tasas de GHz en base a serializadores [32, 33, 34, 35].

Por otro lado, sistemas entrelazados requieren detecciones de estados en tiempos simultáneos, lo que implica que el ruido electrónico en las cuentas experimentales juegan un papel fundamental en la evaluación de estos. Por esto, este tipo de dispositivos embebidos han sido ampliamente aplicados a procesamiento de detecciones en coincidencias (CC).

1.3. Propuesta

En este trabajo de tesis se propone utilizar las características de muestreo por sobre los GHz utilizadas en [32, 33, 34, 35], para generar contadores con resolución superior a $1ns$, logrando disminuir el jitter electrónico y evitar cuentas accidentales en una ventana de detección de coincidencias.

Nuestra propuesta de trabajo incluye implementar la configuración hug, utilizando fibra óptica instalada en laboratorio y terreno, proporcionando una configuración para futuras pruebas utilizando el protocolo Ekert91. Para esto, se debe implementar control activo en el enlace, y optimizar la visibilidad de estados cuánticamente entrelazados, disminuyendo el error por dispositivos electrónicos en la medición de estados.

Por otro lado, en base a semi-independencia sobre los dispositivos [36], se propone diseñar y desarrollar un sistema electrónico en base a lógica programable, para implementar un protocolo propuesto por Pawlowski, el cual bloquearía la correlación entre dos o más QRNG, logrando generar números aleatorios privados.

Además, se propone integrar un protocolo QKD de altas dimensiones, sobre un sistema automático basado en lógica programable. Esta configuración se basará en sistemas de preparación-medida de estados cuánticos con alta-dimensión, los cuales serán transmitidos sobre enlaces de fibra óptica multicore [37].

1.4. Hipótesis

Por lo expuesto anteriormente presentamos la siguiente hipótesis:

Diseñar sistemas electrónicos avanzados en electrónica comercial de bajo costo pueden habilitar sistemas cuánticos que requieren alta precisión en sincronismo, disminución controlada de ruidos y perturbaciones electrónicas, mejorando parámetros como la visibilidad de estados cuánticos sobre enlaces de larga distancia.

1.5. Objetivos

En base a la hipótesis se proponen los siguientes objetivos:

1.5.1. Objetivo general

- Diseñar y construir sistemas electrónicos avanzados en dispositivos embebidos comerciales de bajo costo, para habilitación de sistemas cuánticos sobre enlaces de larga distancia.

1.5.2. Objetivos específicos

1. Aplicar técnicas de control en FPGA comercial, para estabilización de fase en tiempo real sobre interferómetro de larga distancia.

2. Caracterizar la visibilidad de estados cuánticos sobre enlaces de larga distancia, en función de la electrónica de detección.

3. Desarrollo de algoritmos avanzados en electrónica embebida para mejorar visibilidad de estados cuánticos.

4. Desarrollo de sistemas automáticos con alta precisión en sincronismo sobre FPGA, para emisión-recepción de estados cuánticos.

5. Desarrollo de control multiparámetro en FPGA, para control de fase en sistemas cuánticos de alta dimensión.

Los objetivos (1)-(4) cumplidos, tienen la finalidad de habilitar sistemas con entrelazamiento energía-tiempo sobre enlaces de fibra óptica, los cuales serán certificados utilizando las desigualdades de Bell. Mientras que con (4) cumplido, desarrollaremos un sistema de integración electrónica para generación de números aleatorios privados, basado en el concepto de semi-independencia sobre los dispositivos. Finalmente con los objetivos (4) y (5) cumplidos, se desarrollará electrónica embebida para sistema QKD de alta dimensión, utilizando fibra multicore.

CAPÍTULO 2

DISTRIBUCIÓN CUÁNTICA DE CLAVES PARA CRIPTOGRAFÍA

Capítulo 2

Distribución cuántica de claves para criptografía

En este capítulo se introducen conceptos de criptografía clásica, para luego utilizando el formalismo cuántico se presenten los principales protocolos aplicados a criptografía cuántica.

2.1. Criptografía

Compartir y proteger información entre entes distantes es un proceso común en el mundo del internet actual. Para esta tarea se utiliza la criptografía clásica, la cual ha sido utilizada desde hace más de 1000 años antes de cristo, generalmente en movimientos políticos y militares [1].

La figura 2.1 muestra un diagrama esquemático para un sistema criptográfico. En éste, un transmisor codifica un mensaje utilizando una clave, obteniendo un criptograma, el cual se enviará al receptor utilizando un canal público. El receptor decodifica el criptograma utilizando la misma clave de codificación, accediendo a la información del mensaje.

Considerando que tanto emisor como receptor conocen la técnica de codificación y decodificación, la seguridad del mensaje dependerá de la clave en cuestión y de cómo se distribuirá entre los usuarios [38]. Entonces, para que un usuario no autorizado acceda a la información, éste deberá obtener la clave del criptograma. Para esto, puede utilizar técnicas de criptoanálisis sobre criptograma capturado del canal público, o interceptando la transmisión de la clave por canales privados.

2.1.1. Técnicas criptográficas

Existen diversas técnicas para cifrar un mensaje, las más antiguas se basaban en la sustitución y transposición de caracteres de un alfabeto [1].

Las técnicas actuales se basan en la codificación binaria de mensajes digitalizados, para esta tarea se utilizan técnicas conocidas como encriptación simétrica y asimétrica.

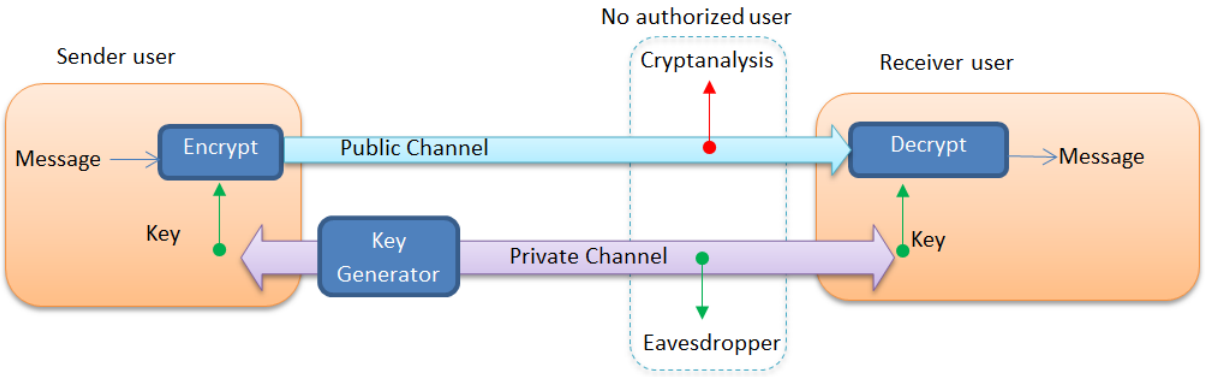


Figura 2.1: Sistema general de comunicación secreta.

Las técnicas simétricas utilizan la misma clave para codificar y decodificar el mensaje, es el caso de *Data-Encryption-Standard* (DES) y *Advanced-Encryption-Standard* (AES), entre otros [39]. En estas técnicas, una cadena de largo fijo es combinada a través de una serie de complicadas operaciones con el texto, el cual es dividido en bloques del mismo largo [39, 6].

Por otro lado los algoritmos asimétricos, o algoritmos con clave pública, utilizan diferentes claves para codificar y decodificar los mensajes. Por ejemplo, la técnica propuesta por Rivest, Shamir y Adleman (RSA), utiliza el producto de dos números primos para generar una clave pública. Con ésta información otro usuario codificará un mensaje, el cual solo será decodificado si se conocen dichos números primos [1].

Finalmente, las técnicas criptográficas actuales se basan en el poder computacional para proteger la información, como por ejemplo la factorización de números primos de muchos dígitos. Sin embargo, las técnicas criptográficas actuales serán vulnerables ante algoritmos ejecutados con computadores cuánticos, los cuales no serán más rápidos, grandes ni pequeños comparados con los computadores actuales, sin embargo tendrán un dramático poder computacional en tareas específicas [2], por ejemplo la habilitación de factorización prima de Shor, la cual podría reducir de un tiempo exponencial a un tiempo polinomial la obtención de factores primos [40], poniendo en riesgo la información privada codificada con RSA.

2.1.2. One-time-pad

Según Shannon, un sistema perfecto de comunicación secreta es el cual tiene un infinito grupo de claves que permiten cifrar mensajes ilimitados [38]. Esto se basa en que las claves constantes y de largo definido están expuestas a ser descifradas con técnicas de criptoanálisis.

La técnica *One-time-pad* [41] es un sencillo método digital, que permite codificar y decodificar mensajes utilizando la misma clave, y se aplica cuando se tiene una clave (K), del mismo tamaño que el mensaje (M), donde K será utilizada solo una vez. Con esto, una simple suma bit a bit (utilizando una compuerta XOR) codificará el texto, obteniendo un criptograma de la forma $E = K \otimes M$. Cuando el criptograma llega al receptor, éste realiza la misma suma obteniendo el mensaje, ya que $E \otimes K = K \otimes M \otimes K = M$. Si la clave es del mismo tamaño que el mensaje, el criptograma no posee información alguna. Sin embargo, el desafío está en distribuir en puntos distantes una clave tan larga como el mensaje, conservando la seguridad de ésta [6].

2.2. Formalismo cuántico

2.2.1. Quantum bit

El bit es un concepto fundamental en la información y computación clásica. La información y computación cuántica se construyen sobre un concepto análogo, denominado *quantum bit* o "qubit". La diferencia entre el qubit y el bit clásico es que el bit tiene dos estados fijos (0 o 1), en cambio el qbit es un sistema de dos estados superpuestos, esto es:

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

donde α y β son complejos, mientras que los estados $|0\rangle$ y $|1\rangle$ forman una base ortonormal para este espacio vectorial. Los estados pueden representar: una polarización, el alineamiento nuclear de un espín en un campo magnético uniforme, el estado de órbita de un electrón en un átomo, etc.

El qubit ($|\psi\rangle$) es un sistema con propiedades cuánticas en un espacio de Hilbert ($\mathcal{H}$), esto es $\mathcal{H} = \{|\psi\rangle\}$. Un espacio $\mathcal{H}$, es un espacio vectorial finito que incluye el producto escalar.

Las posibles bases en un espacio $\mathcal{H}$ pueden escribirse como: $\{|\psi\rangle_i\}$ con $i \in [0, 1, 2.. ..dim(\mathcal{H}) - 1]$. Por ejemplo: un espacio de Hilbert con dimensión 2 puede tener como base $|\psi\rangle_1 = \{|0\rangle, |1\rangle\}$, donde $|0\rangle$ es un estado ortogonal a $|1\rangle$. Geométricamente el qubit debe estar normalizado con largo 1 ($\alpha^2 + \beta^2 = 1$), con esto la ecuación 2.1 se puede reescribir como:

$$|\psi\rangle = e^{i\varphi}\left(cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}sin(\frac{\theta}{2})\,|1\rangle\right), \tag{2.2}$$

donde θ, ϕ y φ son números reales. La fase global $e^{i\varphi}$ puede ser ignorada, debido a que no tiene efectos observables. Por esta razón podemos efectivamente escribir:

$$|\psi\rangle = cos(\frac{\theta}{2})\,|0\rangle + e^{i\phi}sin(\frac{\theta}{2})\,|1\rangle\,. \tag{2.3}$$

Los valores de θ y ϕ definen un punto sobre una esfera tridimensional. Esta esfera frecuentemente es llamada *Esfera Bloch*, cuya representación gráfica se muestra en la figura 2.2. Esta esfera provee un amplio significado de la visualización de estados de un qubit individual (ver Apéndice B), y frecuentemente sirve como una herramienta de pruebas en computación e información cuántica [42].

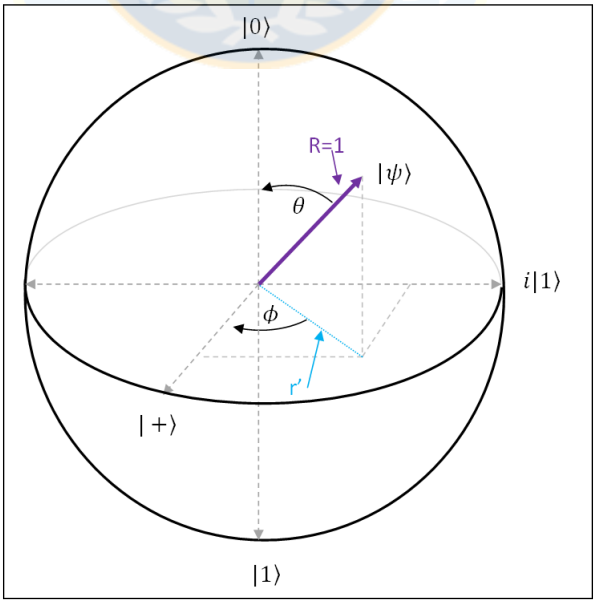


Figura 2.2: Esfera Bloch

2.2.2. Sistemas multidimensionales

Cuando los sistemas tienen alta dimensión ($dim\{\mathcal{H}\} > 2$), estos son conocidos como $qudits$. Sin embargo, los de dimensión tres y cuatro pueden nombrarse $qutrit$ y $quartit$ (o $ququart$) respectivamente. El qudit se escribe como:

$$\begin{aligned} |\psi\rangle &= C_0 |0\rangle + C_1 |1\rangle + ... + C_{dim(\mathcal{H})-1} |dim(\mathcal{H}) - 1\rangle , \\ &= \sum_{i=0}^{dim(\mathcal{H})-1} C_i |i\rangle . \end{aligned} \tag{2.4}$$

El qudit dual al qudit de la ecuación 2.4, está dado por:

$$\langle\psi| = \sum^{dim(\mathcal{H})} C_i^* \langle i| , \tag{2.5}$$

donde C_i es complejo y C_i^* son sus complejos conjugados.

Se define el producto escalar entre dos qudit, como la multiplicación entre el primer qudit y su dual del segundo, esto es:

$$\begin{aligned} \langle\psi|\psi\rangle &= (\sum^{dim(\mathcal{H})} C_i^* \langle i|)(\sum^{dim(\mathcal{H})} C_j |j\rangle), \\ &= \sum_{i=0}^{dim(\mathcal{H})} \sum_{j=0}^{dim(\mathcal{H})} C_i^* C_j \langle i| |j\rangle . \end{aligned} \tag{2.6}$$

Como los estados son ortogonales ($\langle i|j\rangle = 0$ con $i \neq j$ y $\langle i|j\rangle = 1$ para $i = j$), la ecuación 2.6 queda como:

$$\langle\psi|\psi\rangle = \sum_{k}^{dim(\mathcal{H})} C_k^* C_k. \tag{2.7}$$

Manteniendo la condición de normalización sobre 2.7, se tiene:

$$\sum_{k}^{dim(\mathcal{H})} C_k^* C_k = 1. \tag{2.8}$$

Entonces, un sistema con dimensión D en un espacio $\mathcal{H}$, se puede expresar como:

$$|\psi\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} |l\rangle \, e^{i\phi_l}, \tag{2.9}$$

donde

$$\begin{aligned} \langle\psi|\psi\rangle &= \frac{1}{\sqrt{D}} \cdot \frac{1}{\sqrt{D}} \left(\langle 0|0\rangle \, e^{-i\phi_0 + i\phi_0} + \cdots + \langle l_D|l_D\rangle \, e^{-i\phi_{l_D} + i\phi_{l_D}} \right), \\ &= \frac{1}{D} \, (D) = 1. \end{aligned} \tag{2.10}$$

2.2.3. Sistemas compuestos

Si tenemos dos sistemas cuánticos, con espacio de Hilbert $\mathcal{H}_1$ y $\mathcal{H}_2$ respectivamente. El resultado de la interacción entre los sistemas producirá un sistema compuesto, dado por: $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ (donde $\otimes$ es el producto tensorial). Al hacer interactuar el qubit de la ecuación 2.1 con otro en su mismos espacio, producirá el siguiente sistema:

$$\begin{aligned} |\psi_c\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \\ &= \alpha_1 \cdot \alpha_2 |0\rangle \otimes |0\rangle + \alpha_1 \cdot \beta_2 |0\rangle \otimes |1\rangle + \beta_1 \cdot \alpha_2 |1\rangle \otimes |0\rangle + \beta_1 \cdot \beta_2 |1\rangle \otimes |1\rangle \\ &= c_{00} |0\rangle |0\rangle + c_{01} |0\rangle |1\rangle + c_{10} |1\rangle |0\rangle + c_{11} |1\rangle |1\rangle . \end{aligned} \tag{2.11}$$

Por normalización $\sum_{i=0}^{1} \sum_{j=0}^{1} \|c_{ij}\|^2 = 1$. Cabe mencionar, que el producto tensorial suele reducirse al multiplicando de los estados ($|0\rangle \otimes |0\rangle = |0\rangle |0\rangle$). Finalmente, un ejemplo de preparación de sistemas compuesto, son los estados entrelazados.

2.2.4. Entrelazamiento

El entrelazamiento es una de las propiedades fundamentales de la MC. Éste se define como un sistema compuesto que no puede ser escrito como un producto de sistemas individuales.

Por otro lado, un sistema ($|\psi\rangle \in \mathcal{H}$) será separable si existen dos subsistemas $|\phi\rangle$ y $|\varphi\rangle \in \mathcal{H}$, tal que $|\psi\rangle = |\phi\rangle \otimes |\varphi\rangle$. Con esto podemos decir, que un sistema compuesto **no separable** es un sistema entrelazado.

Por ejemplo, al considerar el sistema $|\psi\rangle = \frac{|0\rangle|1\rangle+|1\rangle|0\rangle}{\sqrt{2}}$, es sencillo ver que éste no permite su factorización, tal como la presentada en la ecuación 2.11, por tanto es un sistema entrelazado [42].

El entrelazamiento es observable en términos de las correlaciones clásicas en subsistemas, las medicines experimentales de este principio frecuentemente utilizan las bases de Bell:

$$|\psi^{\pm}\rangle = \frac{|0\rangle\,|1\rangle \pm |1\rangle\,|0\rangle}{\sqrt{2}}, \tag{2.12}$$

$$|\phi^{\pm}\rangle = \frac{|0\rangle\,|0\rangle \pm |1\rangle\,|1\rangle}{\sqrt{2}}. \tag{2.13}$$

Utilizando las bases de Bell, las mediciones sobre $|\psi^{\pm}\rangle$ serán anti-correlacionadas, mientras que en $|\phi^{\pm}\rangle$ serán altamente correlacionadas.

2.2.5. Mutually unbiased bases

Una herramienta para sistemas QKD, son las *mutually unbiased bases* (MUB). Por definición dos bases $V = |v_i\rangle$ y $W = |w_j\rangle$ serán mutuamente imparciales, si el producto interno de todos sus elementos tienen la misma magnitud, esto es $|\,\langle v_i|w_j\rangle\,| = 1/\sqrt{N}$ para todo i, j, donde N es la dimensión del sistema. Esta estructura permite la discriminación de estados en V, si la medición se realiza con el operador de dicha MUB (O_V). Sin embargo, al realizar la medición de estados en W con el operador O_V, el resultado tendrá probabilidad $p = \langle w_j|\, O_V^{\dagger} O_V\, |w_j\rangle = 1/N$ de ser cualquier estado de la segunda MUB, mostrando una **indeterminación del estado medido**. Wootters demostró que en un espacio $\mathcal{H}$ de dimensión N, se pueden encontrar $(N+1)$ MUBs[43].

Un ejemplo simple de MUBs, son bases para $N = 2$ descritas como:

$$\begin{aligned} R &= \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}, \qquad D = \left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}, \\ C &= \left\{ \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}, \end{aligned} \tag{2.14}$$

donde $|r_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, y puede representar cualquier estado cuántico. Las tres MUBs, junto a la identidad, forman parte de las conocidas matrices de Pauli [42].

De la ecuación 2.14, podemos corroborar la imparcialidad de un estado en la base R y los estados de la base D, resultando:

$$|\langle r_0|d_j\rangle| = \left| \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right| = \left| \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right| = \tfrac{1}{\sqrt{2}}. \tag{2.15}$$

Para observar un estado $|v_i\rangle$ de una base V, podemos generar un operador cuántico de medición descrito como $O = |v_i\rangle \langle v_i|$. Por ejemplo, al utilizar el estado $|r_0\rangle$ (ver ecuación 2.14), tenemos:

$$O_{r_0} = |r_0\rangle \langle r_0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{2.16}$$

La probabilidad de observar dicho estado y su ortogonal (en la misma MUB), está dado por:

$$\begin{aligned} p(r_0) &= \langle 0| O_{r_0}^\dagger O_{r_0} |0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1, \\ p(r_1) &= \langle 1| O_{r_0}^\dagger O_{r_0} |1\rangle = \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0. \end{aligned} \tag{2.17}$$

Por último, al utilizar el operador resultante en la ecuación 2.16, con estados de las bases D y C se tiene:

$$\begin{aligned} p(d_0) &= \langle d_0| O_{r_0}^{\dagger} O_{r_0} |d_0\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{1}{2}, \\ p(c_0) &= \langle c_0| O_{r_0}^{\dagger} O_{r_0} |c_0\rangle = \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \tfrac{1}{2}. \end{aligned} \tag{2.18}$$

En resumen, al utilizar operadores de medición de una base V sobre los estados de la misma base se obtendrá una probabilidad máxima de discriminación. Por el contrario, al utilizar operadores de una base V con estados de otra base W, ambas mutuamente imparciales (MUB), no se obtendrá información alguna del estado $|w_j\rangle$ medido, ya que la probabilidad resultante será la misma independiente del estado $|w_j\rangle$ observado.

2.3. Distribución cuántica de claves

2.3.1. Protocolo BB84

El principal protocolo de distribución cuántica de claves del tipo *preparar-y-medir*, es conocido como BB84 [7]. Su estructura se basa en la utilización de al menos dos MUBs, y puede ser aplicado a cualquier sistema cuántico multidimensional ($dim(\mathcal{H}) \geq 2$). Las MUBs son generadas en función de propiedades cuánticas, tales como polarización, fase, Spin, entre otros.

Por ejemplo, las MUBs representadas en la ecuación 2.14 pueden ser generadas utilizando polarización rectangular ($|\psi_R\rangle$), diagonal ($|\psi_\pm\rangle$) y circular ($|\psi_\pm i\rangle$). Con esto, si $|0\rangle$ representa un estado en polarización vertical, entonces $|1\rangle$ representará la horizontal. Los estados diagonales, son formados utilizando una superposición entre los estados rectangulares. Entonces, el estado $45°$ o $|+\rangle$, está dado por $|+\rangle = \frac{1}{\sqrt{2}} \cdot [|0\rangle + |1\rangle]$, y el estado $-45°$ estará dado por $|-\rangle = \frac{1}{\sqrt{2}} \cdot [|0\rangle - |1\rangle]$. En general las MUBs tienen estructura de estados superpuestos, los cuales por la propiedad de superposición cuántica no pueden ser clonados [5].

El protocolo BB84 se basa en la unión de dos puntos separados a través de un canal unidireccional, donde el transmisor (Alice) elige aleatoriamente (de un conjunto de dos MUBs), un estado que enviará a un receptor (Bob). El receptor realiza una medición cuántica al estado recibido, eligiendo aleatoriamente proyectores de una base. Cuando las bases coinciden, se obtienen medidas perfectamente correlacionadas (ver ecuación 2.17), caso contrario los resultados del proceso de medición serán aleatorios (ver ecuación 2.18). Después de una sesión de N eventos, Alice y Bob anuncian las bases de generación y medición, descartando las mediciones de bases *no-coincidentes*. Para esto, se utiliza un canal clásico entre los entes.

Cuando un oyente no autorizado (Eva) intercepta parte de la información transmitida, las mediciones son perturbadas, generando un error que puede ser detectado estimando la tasa de errores de bits cuánticos (QBER), el cual se estima como:

$$QBER = \frac{N_{bad}}{N_{Ok} + N_{Bad}}, \tag{2.19}$$

donde N_{Ok} y N_{bad} corresponden al número de estados correctamente detectados y los erróneos respectivamente. Si Eva detecta parte de la clave generada, ésta deberá devolver un estado para no ser detectado. Como es un estado cuántico superpuesto, al momento de la detección el estado es destruido. Esto implica, que Eva deberá enviar un estado de acuerdo con sus resultados. Sin embargo, como la emisión se realiza utilizando MUBs, Eva no sabrá si midió con la base correcta. Por lo tanto, el estado que ésta devolverá puede no corresponder a la base original.

Alice y Bob hacen comparación de bases, esperando que cuando las bases coincidan todos los estados sean correctamente detectados (QBER=0). Como Eva envía estados sin conocer la base, éste parámetro aumenta su magnitud, delatando la intromisión del espía. Debido a perturbaciones propias del sistema, siempre hay mediciones erróneas (QBER>0), sin embargo se han establecido umbrales para el QBER, los que permiten detectar la intromisión de Eva en sistemas expuestos a condiciones ambientales[44]. Con lo anterior, si el QBER está bajo el umbral: la clave se mantiene, caso contrario se desecha.

Una vez obtenida la clave, Alice y Bob aplican algoritmos de corrección de error obteniendo una clave idéntica en ambos puntos [6]. Finalmente, para reducir la posible información adquirida por Eva, se ejecutan protocolos de amplificación de privacidad [45].

Con los resultados del protocolo anterior, Bennett en 1992 propuso la generación del protocolo B92, el cual utiliza sólo dos estados de dos diferentes MUBs [8]. Sin embargo, la utilización de sólo dos estados no es una solución óptima, debido a que al reducir los estados del sistema el espía puede utilizar la técnica *Unambigue Quantum state discrimination*, propuesta por Ivanovic, Dieks y Peres [46, 47, 48], la cual logra discriminar sin error entre dos estados no-ortogonales con cierta probabilidad.

2.3.2. QKD en altas dimensiones

Los sistemas de alta dimensión han sido ampliamente utilizados en comunicaciones digitales clásicas, como una forma de maximizar la eficiencia del canal de comunicación. Sin embargo, la utilización de estados de alta-dimensión en información cuántica tienen la misión de incrementar la seguridad, además su utilización permite tolerar más ruido que los estados de dos dimensiones (QBER mayor) [44]. Estos sistemas han sido generados utilizando; energía tiempo [49], momento angular orbital [50], momento transversal [9], entre otros.

Uno de los trabajos de interés, es la generación de QKD utilizando dimensión 16 [9]. Este trabajo es un sistema QKD en base al protocolo BB84, que utiliza modulación en momento transversal, para obtener estados con dimensión 16 (MUBs de 16x16). El qudit utilizado tiene la forma: $|\psi\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{l_D-1} |l\rangle \, e^{i\phi_l}$, donde ϕ_l es la fase de cada estado, la cual es previamente definida en las MUBs utilizadas.

La fase es modulada utilizando un esquema que contempla dos *spatial light modulator* (SLM), donde primeramente se generan rendijas espaciales, permitiendo la transmisión espacial controlada de un fotón, para luego incorporarle una fase dependiente del camino recorrido por éste. Los SLM son dispositivos activos controlados por un puerto VGA, la principal ventaja es que la modulación generada puede ser aplicada sin afectar el alineamiento óptico de la configuración experimental [51].

Aunque en principio la modulación utilizando SLM, podría generar centenares de estados (utilizando modulación por pixel), la tasa de generación de éste se limita a los drivers de control. El problema de la utilización de computadores, es la latencia en la generación de la imagen. Por esto, Etcheverry utiliza electrónica dedicada para aumentar la tasa a 30 qudit por segundo [9].

Por lo dicho anteriormente; ¿Es óptimo utilizar qudit en un protocolo QKD?, y por otro lado ¿Será posible aumentar la tasa de comunicación utilizando altas dimensiones?.

En este trabajo proponemos abordar la idea de generar ququart, utilizando un espejo deformable el cual podrá aumentar la taza a 1000 ququart por segundo, con las ventajas de seguridad aportadas por un sistema multidimensional.

En telecomunicaciones siempre se intenta aumentar la tasa de transmisión en una conexión, la utilización de multiplexación por división espacial ha aumentado el interés en la fibra multicore, haciendo factible el desarrollo de conexiones a larga distancia con ésta [37].

Con lo anterior, a parte de aumentar la tasa de emisión, se propone generar un enlace buscando la mayor separación espacial posible dentro del laboratorio. Para abordar este objetivo se propone la utilización de fibra multicore, la cual puede ser utilizada como canales independientes en una misma fibra, y cuyas perturbaciones o variaciones de los estados se generarán de igual forma en todos los núcleos de la fibra, dando estabilidad en la interferencia de salida.

2.3.3. Protocolo QKD de Artur Ekert

El protocolo de Ekert [11] es un método donde la seguridad de QKD depende completamente de la mecánica cuántica, específicamente del entrelazamiento cuántico.

El entrelazamiento es un fenómeno en el cual dos o más partículas muestran una alta correlación en sus propiedades, al medirlas en tiempo simultáneo y a una distancia simétrica entre la fuente y los usuarios, independientes del largo de la separación y tiempo después de su generación. Con esto, si dos usuarios distantes midieran cuánticamente partículas entrelazadas, las que fueran enviadas en distinta dirección a dichos puntos, estos obtendrían información correlacionada, si las mediciones se realizan en tiempos simultáneos. Por el contrario, si las mediciones se realizan en tiempos no simultáneos, los resultados serán completamente aleatorios.

Al realizar N eventos se generaría una cadena de datos los cuales pueden ser utilizados como claves para criptografía. Luego, se utilizan las desigualdades de Bell [12, 13], para verificar que los estados estén entrelazados.

El método anterior mantiene la privacidad de la distribución de claves, ya que la generación no depende de dispositivos ópticos, ni utiliza dispositivos activos, tales como generadores de aleatoriedad. Por otro lado, la utilización de estados entrelazados, hace que la posible información que pueda capturar un espía no contenga información, debido a que el resultado de medición en Alice y Bob se obtendrá en el instante de la medición y no antes.

Por tanto, con esta acción el espía robará información que no existe aún, además al devolver esta partícula absorbida, ésta no estará entrelazada. Luego, al evaluar las desigualdades de Bell utilizando las partículas anteriores, el resultado permitiría detectar la intromisión del espía. Dicha desigualdad, se explica con detalle en el siguiente capítulo.

CAPÍTULO 3

DESIGUALDADES DE BELL

Capítulo 3

Desigualdades de Bell

En este capítulo se presenta la desigualdad de Bell y unas generalizaciones. Para esto, se muestra como la mecánica cuántica (MC) explica matemáticamente la relación entre dos partículas entrelazadas, cuyo impacto produce (en base a críticas), una herramienta para comprobar experimentalmente este fenómeno.

Formalmente, el entrelazamiento implica la existencia de estados globales de un sistema compuesto, el cual no puede escribirse como un producto de subsistemas individuales (ver sección 2.2.4). Éste es un fenómeno en el cual dos o más partículas muestran una alta correlación en sus propiedades, sólo al medirlas en distancia simétrica y tiempos simultáneos después de su generación, pero cuando la medición se realiza en diferentes condiciones no existe correlación alguna. Esto implica dependencia sobre la medición, y que los resultados son determinados en el momento de la medición y no están predefinidos [52]. Para evaluar un sistema entrelazado se utiliza un experimento que incluye un emisor (Charlie), y dos receptores Alice y Bob. Charlie prepara un par de partículas entrelazadas, y envía una de éstas a Alice y la otra a Bob. Por su parte, Alice y Bob observan las propiedades de la partícula utilizando operadores (aparatos), los cuales pueden medir dos diferentes propiedades. La propiedad a medir es elegida de forma aleatoria e independiente, y cada medición hecha por un ente no afectan la medición del segundo. En la figura 3.1 se muestra dicho experimento, donde las bases son $[a_1, a_2]$ para Alice y $[b_1, b_2]$ para Bob. Éstas habilitan los aparatos $A()$ y $B()$ en los dos puntos respectivamente, cuya salida o resultado serán valores discretos $+1$ o -1 [13].

3.1. Medición cuántica del entrelazamiento

El sistema preparado por Charlie será un estado entrelazado puro, descrito por:

$$|\psi\rangle = \frac{|0\rangle\,|1\rangle + |1\rangle\,|0\rangle}{\sqrt{2}}. \tag{3.1}$$

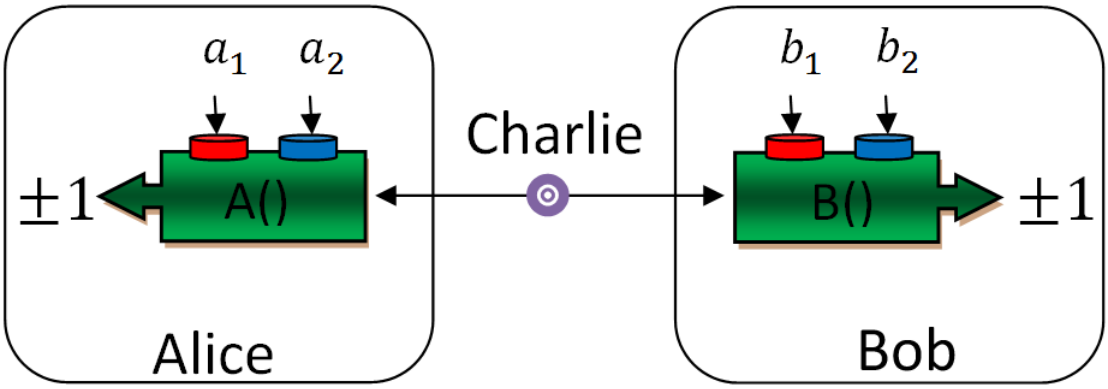


Figura 3.1: Configuración experimental, para explicar el entrelazamiento cuántico.

Las propiedades a medir pueden ser: polarización, dirección de un Spin, fase, etc. Éstas se describen utilizando MUBs, las cuales en dimensión 2 serán las matrices de Pauli [42].

Definimos las propiedades a medir en Alice como $\hat{\alpha} = [a_1, a_2, a_3]$ y en Bob $\hat{\beta} = [b_1, b_2, b_3]$. Los operadores de medición en Alice y en Bob, denominados como $A()$ y $B()$ respectivamente, estarán dados por:

$$\begin{aligned} O_a &= a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3, \\ O_b &= b_1\sigma_1 + b_2\sigma_2 + b_3\sigma_3. \end{aligned} \tag{3.2}$$

Por el postulado 4 de la MC (ver Apéndice C), el operador para medir la correlación entre las partículas entrelazadas, está dado por el operador conjunto $O_a \otimes O_b$, descrito por:

$$\begin{aligned} O_a \otimes O_b &= (a_1\sigma_1 + a_2\sigma_2 + a_3\sigma_3) \otimes (b_1\sigma_1 + b_2\sigma_2 + b_3\sigma_3), \\ &= \sum_{i,j=1}^{3} a_i b_j \sigma_i \otimes \sigma_j. \end{aligned} \tag{3.3}$$

Además, por el postulado 3 el valor esperado para una medición cuántica utilizando el operador compuesto en 3.3, está dado por:

$$\langle E(\alpha,\beta)\rangle = \langle\psi| O_a \otimes O_b |\psi\rangle = \langle\psi| \sum_{i,j=1}^{3} a_i b_j \sigma_i \otimes \sigma_j |\psi\rangle . \tag{3.4}$$

Ahora, al desarrollar (3.4) considerando el sistema de (3.1), se tiene:

$$\begin{aligned}\langle E(\alpha,\beta)\rangle &= \sum_{i,j=1}^{3} a_i b_j \langle\psi|\, \sigma_i \otimes \sigma_j \,|\psi\rangle\,, \\ &= \left(a_1 b_1 \langle\psi|\, \sigma_1 \otimes \sigma_1 \,|\psi\rangle + ... + a_3 b_3 \langle\psi|\, \sigma_3 \otimes \sigma_3 \,|\psi\rangle\right), \\ &= \frac{1}{2}\left(a_1 b_1 \{-2\} + a_2 b_2 \{-2\} + a_3 b_3 \{-2\}\right), \\ &= -a_1 b_1 - a_2 b_2 - a_3 b_3 = -\hat{\alpha}\cdot\hat{\beta} = -cos(\theta_{\alpha\beta}).\end{aligned} \tag{3.5}$$

Esta ecuación describe el comportamiento de dos partículas entrelazadas, donde su correlación a distancia está dada por el ángulo entre éstas. Es importante señalar que el experimento en la figura 3.1 considera 2 bases. Aunque el resultado de 3.5 se obtuvo con dimensión 3, el lector puede realizar el cálculo utilizando sólo dos y obtendrá la misma relación.

Los investigadores Einstein, Podolsky, y Rosen no estaba de acuerdo con la acción fantasmal del entrelazamiento (spooky). Ellos aceptaban como una teoría completa, la que se pueda aplicar a sistemas cuyas propiedad se puedan predecir sin perturbar al sistema (lo cual es opuesto a las propiedades del entrelazamiento), infiriendo que la mecánica cuántica no es una teoría completa [53]. Para generar una teoría completa proponen la existencia de *variables ocultas*.

Utilizando estos argumentos, John Bell muestra que la teoría de variables ocultas no locales puede reproducir todas las predicciones cuánticas [12]. Para esto, Bell define λ como una o varias variables ocultas. Con esto, el resultado de una medición hecha por Alice se expresará como una medición dependiente de λ.

3.2. Desigualdad de CHSH

En 1969 Clauser y su grupo generalizan el teorema de Bell, logrando obtener una expresión de desigualdad aplicada a experimentos realizables [13]. Esta desigualdad actualmente es conocida como la desigualdad CHSH, y su ventaja es que puede ser aplicada a experimentos utilizando pares de fotones.

Para las mediciones en el esquema de la figura 3.1, se utilizan cuatro bases $\{a_1, a_2, b_1, b_2\}$, y cada partícula es detectada por un observador $A()$ y $B()$ en Alice y Bob respectivamente. Se asume que las partículas son generadas por una fuente físicamente desligada de la elección de bases en la medición, y que la densidad de probabilidad $p(\lambda)$ es independiente de las bases. Con esto, definimos el valor esperado entre las lecturas correlacionadas de Alice y Bob como:

$$E(a,b) = \int A(a,\lambda)B(b,\lambda)\rho(\lambda)d\lambda. \tag{3.6}$$

Si las salidas del experimento están dadas por $A(a_i,\lambda) = \pm 1$ y $B(b_j,\lambda) = \pm 1$, entonces el valor conjunto de las mediciones es:

$$A(a_i,\lambda)B(b_j,\lambda) = \pm 1. \tag{3.7}$$

Al evaluar la correlación entre a_1 y sus posibles medidas utilizando b_1 y b_2, se tiene:

$$E(a_1,b_1) - E(a_1,b_2) = \int A(a_1,\lambda)B(b_1,\lambda)\rho(\lambda)d\lambda - \int A(a_1,\lambda)B(b_2,\lambda)\rho(\lambda)d\lambda, \tag{3.8}$$

donde

$$\int \rho(\lambda)d\lambda = 1. \tag{3.9}$$

Sumando la expresión $\pm \int A(a_1,\lambda)B(b_1,\lambda)A(a_2,\lambda)B(b_2,\lambda)\rho(\lambda)d\lambda$ a la ecuación 3.8, se obtiene:

$$\begin{aligned}
&E(a_1,b_1) - E(a_1,b_2)\\
&= \int \left[A(a_1,\lambda)B(b_1,\lambda) - A(a_1,\lambda)B(b_1,\lambda)A(a_2,\lambda)B(b_2,\lambda)\right]\rho(\lambda)d\lambda\\
&- \int \left[A(a_1,\lambda)B(b_2,\lambda) - A(a_1,\lambda)B(b_1,\lambda)A(a_2,\lambda)B(b_2,\lambda)\right]\rho(\lambda)d\lambda,\\
&= \int A(a_1,\lambda)B(b_1,\lambda)[1 - A(a_2,\lambda)B(b_2,\lambda)]\rho(\lambda)d\lambda\\
&+ \int -A(a_1,\lambda)B(b_2,\lambda)[1 - A(a_2,\lambda)B(b_1,\lambda)]\rho(\lambda)d\lambda,
\end{aligned} \tag{3.10}$$

$$|E(a_1,b_1)-E(a_1,b_2)| \leq \int |A(a_1,\lambda)B(b_1,\lambda)|\,[1-A(a_2,\lambda)B(b_2,\lambda)]\rho(\lambda)d\lambda + \int |-A(a_1,\lambda)B(b_2,\lambda)|\,[1-A(a_2,\lambda)B(b_1,\lambda)]\rho(\lambda)d\lambda. \tag{3.11}$$

Utilizando el valor absoluto de (3.7) en (3.11), se tiene:

$$\begin{aligned} |E(a_1,b_1)-E(a_1,b_2)| &\leq \int [1-A(a_2,\lambda)B(b_2,\lambda)]\rho(\lambda)d\lambda \\ &\quad + \int [1-A(a_2,\lambda)B(b_1,\lambda)]\rho(\lambda)d\lambda, \\ &\leq \int \rho(\lambda)d\lambda - \int A(a_2,\lambda)B(b_2,\lambda)\rho(\lambda)d\lambda \\ &\quad + \int \rho(\lambda)d\lambda - \int A(a_2,\lambda)B(b_1,\lambda)\rho(\lambda)d\lambda. \end{aligned} \tag{3.12}$$

Por ultimo, considerando (3.9) y (3.6) en 3.12 tenemos:

$$\begin{aligned} |E(a_1,b_1)-E(a_1,b_2)| &\leq 2-[E(a_2,b_2)+E(a_2,b_1)]\,, \\ |E(a_1,b_1)-E(a,b_2)|+E(a_2,b_2)+E(a_2,b_1) &\leq 2. \end{aligned} \tag{3.13}$$

La expresión de la ecuación 3.13, se conoce como la desigualdad de CHSH [13] y formalmente es presentada como:

$$S = E(a_2,b_2)+E(a_2,b_1)+E(a_1,b_1)-E(a_1,b_2) \leq 2. \tag{3.14}$$

3.3. Contradicción cuántica evaluando las desigualdad CHSH

La ecuación 3.14 se construye bajo la hipótesis que la correlación en las medidas observadas dependen de variables ocultas [13], obteniendo una desigualdad que limita los valores de las posibles interacciones en el experimento EPR.

Sin embargo, utilizando los resultados de correlación cuántica dado por el mismo experimento $E(\alpha, \beta) = -cos(\theta_{\alpha\beta})$ (ver ecuación 3.5), sobre la desigualdad descrita en (3.14), se obtiene:

$$\begin{aligned} S &= E(a_2, b_2) + E(a_2, b_1) + E(a_1, b_1) - E(a_1, b_2), \\ &= -cos(\theta_{a_2,b_2}) - cos(\theta_{a_2,b_1}) - cos(\theta_{a_1,b_1}) + cos(\theta_{a_1,b_2}). \end{aligned} \tag{3.15}$$

Eligiendo $-cos(\theta_{a_2,b_2}) = -cos(\theta_{a_2,b_1}) = -cos(\theta_{a_1,b_1}) = cos(\theta_{a_1,b_2}) = \frac{\sqrt{2}}{2}$, y reemplazando en la ecuación 3.15, se obtiene $S = 2\sqrt{2}$, cuyo valor es superior al limite impuesto por las variables ocultas de Bell. Este descubrimiento genera un límite entre la física determinista y la mecánica cuántica. El cual se ha convertido en una herramienta, debido a que su violación permite evaluar el entrelazamiento cuántico en sistemas experimentales ($S > 2$).

3.4. Generalización de la desigualdad de CHSH (I-Chained)

La desigualdad de Bell es aplicada a un par de sistemas de dos estados, y se compone de la observación en correlación existente entre los dos sistemas. Braunstein y Caves [14] proponen la generalización de dicha desigualdad de dos formas.

1. En base a la desigualdad de CHSH obtienen una correlación en serie de las desigualdades de Bell para dos sistemas.

2. Se formulan desigualdades, las cuales están escritas en termino de la información obtenida en experimentos con más de dos estados.

Con lo anterior, la desigualdad de *I-Chained* para n estados, se obtuvo con la siguiente forma:

$$S_{Ich}(n) = \sum_{i=1}^{n} E(a_i, b_i) + E(a_{i+1}, b_i) \leq 2n - 2, \tag{3.16}$$

donde $E(a_i, b_i) = \langle A_i B_i \rangle$. La evaluación de esta serie se realiza con la siguiente condición $A_{n+1} \equiv -A_1$, entonces al evaluar S_{Ich} con $n = 2$ se obtendrá la desigualdad de CHSH [54], esto es:

$$\begin{aligned} S_{Ich}(2) &= \sum_{i=1}^{2} E(a_i, b_i) + E(a_{i+1}, b_i) \leq 2 \cdot 2 - 2, \\ &= E(a_1, b_1) + E(a_2, b_1) + E(a_2, b_2) + E(a_{2+1}, b_2) \leq 2, \\ &= E(a_1, b_1) + E(a_2, b_1) + E(a_2, b_2) - E(a_1, b_2) \leq 2. \end{aligned} \tag{3.17}$$

3.5. Loopholes en la mecánica cuántica

Actualmente, en determinados experimentos la mecánica cuántica viola las desigualdades de Bell, evidenciando el fenómeno de entrelazamiento. Sin embargo, aún existen circunstancias que obligan a tomar *supuestos extras* para lograr la violación, evitando que los experimentos tengan validez absoluta. Estas circunstancias son conocidas como loopholes, los cuales abren la posibilidad de que el realismo local salga adelante en los experimentos de desigualdad [15]. Los loopholes más conocidos son de localidad y de eficiencia de detección.

Según el loophole de localidad, si la comunicación entre dos posiciones es posible, entonces el modelo de variables ocultas locales es válido. Debido a que cuando se mide en un punto, una señal puede viajar al otro con la información de la primera medición. El primero en cerrar este loophole fue Aspect en 1982 [55], Sin embargo este loophole se cierra estrictamente por Weihs en 1998 [56]. En este experimento se utiliza una separación de 400 metros ($1{,}3\mu s$) y se argumenta que el retraso total entre la óptica y la electrónica fue de $100ns$. Bajo estas condiciones, se obtuvo un valor $S = 2{,}73 \pm 0{,}02$, violando la desigualdad de CHSH por más de 30 desviaciones estándar.

Por otro lado, el loophole de eficiencia de detección [15] consiste en que algunas partículas no son medidas, perdiendo información del sistema. Esto implicaría, que la falta de información habilita la violación de las desigualdades de Bell. Sin embargo, Matsukevich el 2008 utilizando una eficiencia de detección del $98\,\%$ sobre iones entrelazados [57], obtienen una fidelidad de $86\,\%$ y un valor $S = 2,22 \pm 0,07$, violando la desigualdad de CHSH por 3 desviaciones estándar, cerrando el loophole de eficiencia de detección.

Los experimentos anteriores realizaron los primeras violaciones cerrando loopholes por separado. Sin embargo, sólo el 2015 Hensen y su grupo logran violar las desigualdades de Bell libre de ambos loopholes [16]. Este resultado es de gran impacto, ya que la utilización de sistemas entrelazados en protocolos QKD, permitirían que la seguridad dependa completamente de la mecánica cuántica. Sin embargo, las partículas entrelazadas utilizadas en [16], hacen aún poco práctica la implementación de este sistema sobre protocolos QKD. Por esto, la implementación de entrelazamiento sobre fotones sigue siendo un desafió atractivo para investigación.

CAPÍTULO 4

SISTEMAS EMBEBIDOS EN COMUNICACIÓN CUÁNTICA

Capítulo 4

Sistemas embebidos en comunicación cuántica

Las mediciones, control y procesamiento de datos para experimentos en información cuántica (QI), deben ser en tiempo real y con resolución en nano segundos. Por este motivo, una solución digital de bajo costo es el empleo de *field programmable gate array* (FPGA) en el desarrollo de sistemas para QI, tales como distribución cuántica de claves (QKD) [22, 23, 24] y unidades contadoras de coincidencias (CCU) [25, 26, 27, 28, 29].

Un FPGA es un arreglo de compuertas y recursos digitales cuya lógica y conexión son completamente configurables, presentando máxima velocidad de información digital entre las celdas interconectadas, además de permitir cambios en el circuito en cualquier momento. Esto, sumado a la utilización de unidades *Intellectual-Property* (IP), integrados en el chip FPGA [30, 31], han permitido diseños de sistemas QKD a tasas de GHz en base a serializadores [32, 33, 34, 35].

Por otro lado, las CCU son utilizadas para evaluar detecciones simultáneas en experimentos con sistemas entrelazados. La precisión en una ventana de coincidencia es fundamental en este tipo de aplicaciones [29], debido a que el ruido electrónico en las detecciones juegan un papel fundamental en el error del sistema.

Aunque la eficiencia de detección, corrientes oscuras y tiempo muerto, son limitaciones propias del detector (foto diodo de avalancha, APD) [58], el jitter electrónico es un ruido presente en los APDs y la electrónica de la CCU. En nuestra hipótesis nos enfocamos en disminuir el error electrónico de la CCU para aumentar la calidad de las detecciones procesadas. Con esto, se reduce el error de detección y por tanto aumenta la fidelidad y/o visibilidad de estados cuánticos, permitiendo que estos parámetros dependan unicamente de la calidad de los detectores y no de factores electrónicos de la CCU.

Uno de los factores de error de detección son las cuentas accidentales, estas son proporcionales al ancho de la ventana de detección en coincidencia. Por esto, utilizando diseños basados en lógica discreta dentro de un FPGA, se ha logrado disminuir esta ventana a pocos

nano segundos [25, 26, 27, 28], e incluso utilizando retrasos, en base a buffer internos, se puede obtener una ventana con resolución inferior a los nano segundos [29]. Aunque estos diseños tienen un gran desempeño, logrando adquirir coincidencias por sobre $160MHz$, la gran mayoría de los detectores utilizados actualmente, no superan una tasa de detecciones de $30MHz$ [58]. Sin embargo, en estos diseños el ancho de la ventana de detección se obtiene exigiendo al máximo los tiempos de operación, obteniendo un ancho de ventana fijo por medición experimental [29, 28].

La propuesta de este trabajo es utilizar retrasos analógicos y serializadores integrados en un FPGA Spartan 6 [31], para aumentar la resolución de procesamiento y por tanto reducir el error electrónico, además de reducir la ventana de detección para disminuir cuentas en coincidencias accidentales.

Con la disminución de cuentas erróneas y accidentales, eventualmente se aumenta la fidelidad cuántica y la visibilidad óptica en sistemas cuánticos. Con esto, por ejemplo se habilitaría la certificación de estados entrelazados utilizando las desigualdades de Bell. Todo esto, bajo una arquitectura que permite visualizar múltiples ventanas de coincidencia en un mismo experimento con resolución de $500ps$, cuyo diseño podría expandirse a $250ps$ por ventana de detección en trabajos futuros.

4.1. Muestreo digital de alta resolución

Para muestrear una señal a alta resolución, en nuestro diseño utilizamos un serializador ISERDES2 incluido en el chip Spartan 6 [31]. Esta unidad obtiene la información binaria de la amplitud analógica a cada $1ns$, permitiendo una conversión serial-a-paralelo con relación 1:8, lo que permite generar cadenas binarias de 8 bits cada $8ns$ ($125Mhz$).

La figura 4.1.a, muestra la digitalización de un pulso $P(t)$ utilizando un serializador, con este dispositivo obtenemos cadenas de 8 bits en un tiempo k, la cual denominaremos $S[k]$.

Para doblar la resolución de trabajo, el pulso $P(t)$ es conectado a una segunda entrada, donde se retrasa un tiempo δ, obteniendo una señal $P(t-\delta)$. Para esto utilizamos una unidad analógica IODELAY2 integrada a un FPGA Spartan 6 [31]. El pulso analógico obtenido $P(t-\delta)$, es conectado a un segundo serializador para obtener un muestreo $M[k]$ (ver figura 4.1.a).

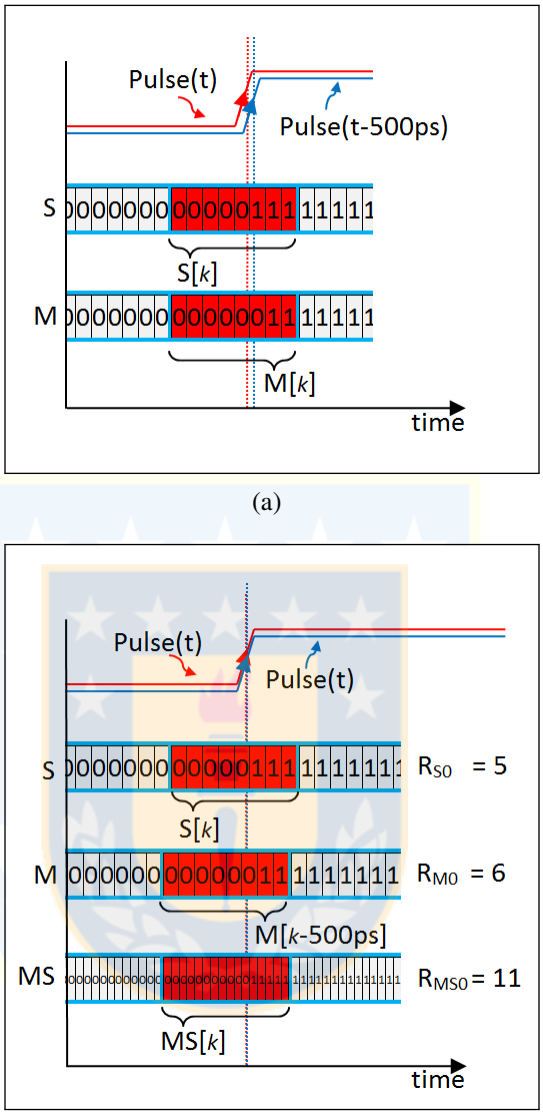


Figura 4.1: Diagrama de muestreo digital. a) Pulsos desfasados por $500ps$. b) La información en $S[k]$ y $M[k-500ps]$ produce un registro $MS[k]$ con mayor resolución.

Como la resolución del serializador es de $1ns$, entonces configuramos la unidad IO-DELAY2 para obtener un retraso de $500ps$. Como las cadenas de 8 bits son muestreadas utilizando serializadores sincronizados entre ellos, la data digital entre $S[k]$ y $M[k]$ estará desfasada en $500ps$. Entonces, al recombinar ambas cadenas se obtiene una tasa de muestreo final equivalente de $2GSPs$, sobre una tercera cadena denominada $SM[k]$. La figura 4.1.b muestra un diagrama de esta operación.

4.2. Arquitectura Contador de coincidencia

La figura 4.2 muestra la arquitectura empleada para nuestra unidad de cuentas en coincidencias. El muestreo de alta resolución descrito en la sección anterior, se muestra en la etapa **Pulse-to-digit**. Aunque podemos procesar directamente la data de alta resolución ($SM[k]$), en este trabajo procesamos cada cadena de 8 bits, obtenida a $1GSPs$, por separado.

Para evitar cuentas falsas, definiremos un arribo como la transición de un estado "0" a un estado "1" con duración mínima de $5ns$ (cinco bits "1" consecutivos). Con esto, si el arribo llega en el bit más significativo de la cadena adquirida de 8 bits ($S[k]$), la siguiente cadena tendrá la forma $S[k] = 11111111$. Luego, solamente necesitamos ver el bit menos significativo de la cadena anterior ($S[k-1] = 00000000$), para cumplir con la restricción de arribo real. Por otro lado, si el arribo llega en el bit menos significativo de nuestra cadena ($S[k] = 00000001$), para obtener el arribo real necesitamos los cuatro bits consecutivos a nuestro muestreo (cuatro bit más significativos de la cadena siguiente $S[k+1] = 11111111$).

En resumen, para obtener un arribo real (cuenta), necesitamos re-ordenar temporalmente las cadenas adquiridas, de tal forma de concatenar el primer bit de $S[k-1]$, los ocho bits actuales $S[k]$ y los cuatro bit siguientes de $S[k+1]$, generando una cadena de 13bits. Según la figura 4.2, la cadena de 13 bits es obtenida del módulo re-arrangement (R-Arr), para luego ser evaluada en el módulo String-to-radius. Estos módulos se encuentran en la etapa **Coincidence-counter** (ver figura 4.2).

4.2.1. Módulo string-to-radius

En este módulo se evalúa el tiempo de llegada de un arribo válido (sucesión 011111), para esto definimos como radio inicial R_0 a la posición del primer bit "1" dentro de $S[k]$. Por ejemplo, si el arribo llega en el bit más significativo de $S[k]$, entonces $R_0 = 0$, mientras que si llega en el menos significativo $R_0 = 7$ (ver figura 4.1.b). Una vez detectado el arribo, se obtiene R_0 y una señal de detección, la cual es utilizada para contabilizar detecciones simples (C_S), y para evaluar una diferencial de radios. Si el pulso se mantiene en alto o está en el flanco de bajada, R_0 decrecerá en $8ns$ por cada ciclo de trabajo (a $125Mhz$).

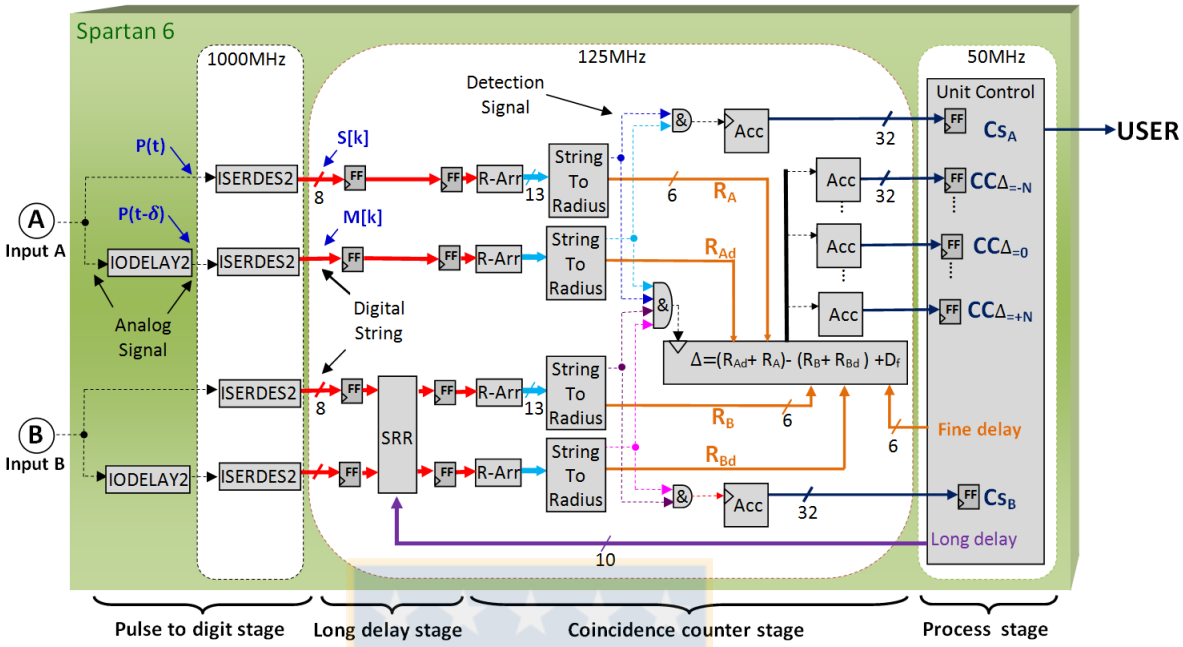


Figura 4.2: Diagrama Arquitectura Contador con resolución de $500ps$. Considerando la entrada "A", dos pulsos analógicos provenientes de esta entrada son desfasados $t_d = 500ps$ utilizando una unidad analógica IODELAY2, que esta integrada a un FPGA Spartan 6. Utilizando unidades ISERDES2, cada señal desfasa es digitalizada a $1GSPs$, obteniendo cadenas digitales de 8 bit separadas por $1ns$. Esta cadena es obtenida cada $8ns$ ($125MHz$), y se reordena temporalmente obteniendo una cadena de 13bits, con la cual se obtiene un radio de arribo en el módulo String-to-radius. De este módulo, una señal de detección es utilizada para contabilizar detecciones simples (C_S) y para evaluar una diferencial de radios. La suma de los radios desfasados con resolución de $1ns$ ($R_A + R_{Ad}$), equivale a un radio con resolución de $500ps$ ($\hat{R}_A$). Finalmente, la diferencia entre $\hat{R}_A$ y$\hat{R}_B$, permite saber cual es la distancia de arribo, donde cero equivale a una cuenta en coincidencia (CC), con ventana de coincidencia cuyo ancho es $500ps$. Por último, utilizando una memoria, las cadenas de la input-A pueden ser retrasadas con respecto a la input-B. Las cuentas finales y parámetros del sistema son evaluados en la etapa de procesos, la cual opera a $50MHz$ y es conectada vía USB a un usuario. En la Figura: (FF) Flip-Flops, (SRR) Shift Ram Register, (R-Arr) reordenador de cadenas, (Acc) Acumulador de 32bits.

Al evaluar los radios obtenidos en las cadenas $S[k]$ y $M[k]$ (cuya resolución es de $1ns$), obtenemos que el radio de $MS[k]$ de $500ps$ es igual a la suma de los radios anteriores, esto es: $R_{MS0} = R_{S0} + R_{M0}$ (ver figura 4.1.b).

Según la figura 4.2, los radios R_S y R_M los obtenemos como R_A y R_{Ad} para la entrada "A", y R_B con R_{Bd} para la entrada "B". Con dichos parámetros, se evalúa la diferencial

entre las combinaciones anteriores ($\Delta = (R_A + R_{Ad}) - (R_B + R_{Bd})$), obteniendo la separación temporal con resolución de $500ps$ entre los pulsos provenientes de las entradas A y B. Dicha diferencial, sólo es ejecutada cuando los arribos en A y B son detectados, esto se determina con la multiplicación de las señales de detección en cada radio.

Los distintos valores para la diferencial Δ, son almacenadas en distintos acumuladores de 32bits, de tal forma de guardar N radios de arribo, los radios son preprocesados y enviados al usuario en la etapa **Process**. El usuario con estos registros obtiene un histograma temporal del arribo en tiempo real, que es equivalente a medir con distintos anchos de ventanas de coincidencia en un mismo experimento.

La arquitectura presentada puede aumentar la resolución a $250ps$, considerando cuatro unidades ISERDES2, cuyas señales provenientes de una única entrada, estén desfasadas por múltiplos de $250ps$, utilizando tres IODELAY2. Con esto, el proceso de obtención de arribos puede ser ejecutado utilizando el mismo módulo String-to-Radius y la diferencial mencionada.

4.2.2. Retraso electrónico para cuentas en coincidencias

En nuestra CCU incluimos dos tipos de retrasos: retraso grueso y retraso fino, los que permitirán compensar retrasos ópticos en las cuentas coincidentes. Como muestra la figura 4.2, las cadenas generadas en el canal "input-A" son retrasadas con respecto a las obtenidas desde "input-B" a través de un Shift-RAM-Register de $1024x8bits$, cuyo índice configurable permite generar un retraso entre $8ns$ y $8\mu s$, todo esto en la etapa **Long-delay**. Este retraso lo denominaremos **retraso-largo**, ya que las cadenas dentro de la memoria tienen un tiempo de muestreo fijo en $8ns$.

Por otro lado, agregamos un retraso fino (D_f) el cual opera directamente en la diferencial, con rango entre 0 y $7{,}5ns$.

Como el diseño presentado permite evaluar tiempos de arribo, dicha electrónica puede ser utilizada en una multiplexación temporal de señales (time-bin). Lo que permitiría medir con sólo dos puertos, múltiples proyecciones cuánticas provenientes de un mismo experimento [59, 60].

4.3. Evaluación del diseño desarrollado

Para evaluar el funcionamiento de nuestro diseño, utilizamos una configuración de pares entrelazados en polarización, generados a través de un cristal PPKTP usado para type-II down-conversion [61]. Los fotones generados son filtrados y separados por un PBS, con una tasa de generación aproximada de $100k$ cuentas por segundo. Utilizamos detectores SPCM-AQRH, con pulsos de $50ns$ y rango de detección entre 400 y $1060nm$. Uno de los detectores se conecta en serie con un generador digital de retrasos (Tektronix AFG3021B), que retrasa la señal eléctrica en pasos de $100ps$. Aquí una ventana de detección en coincidencia t_w, tendrá la forma:

$$t_w = nt_r + d_w, \tag{4.1}$$

donde n es entero mayor a cero y determina el ancho de la ventana, t_r es la resolución de trabajo (en nuestro caso $t_r = 500ps$), y d_w es una variación este ancho producto del ruido electrónico (*Skew*). Clásicamente la ventana de detección es excitada por un pulso eléctrico en la entrada "A", entonces al dejar como referencia el arribo de esta misma señal, la entrada en "B" presentará un ruido electrónico con distribución gaussina [62] con respecto a la referencia en "A". Este ruido electrónico básicamente es el jitter y el error de resolución del sistema, y lo modelamos de la forma:

$$g(t_d) = N\mathrm{e}^{-\frac{(t_d-\mu)^2}{2\sigma^2}}, \tag{4.2}$$

donde N son las cuentas muestreadas en un periodo, t_d es el tiempo de retraso entre la entrada "B" respecto a la entrada "A", μ es la media temporal de la gaussiana y σ es la desviación estándar del error electrónico.

Bajo las condiciones anteriores, el dispositivo electrónico presentará una detección en coincidencia sólo cuando $t_d \leq t_w$, esta función se describe como:

$$h(t_d) = \begin{cases} 1 & 0 \leq t_d \leq t_w \\ 0 & \text{Other case} \end{cases} \tag{4.3}$$

Realizando un barrido de t_d cada N cuentas en el esquema mencionado, se obtendrá la distribución de las cuentas en coincidencias sobre t_w. El resultado experimental se muestra en la figura 4.3, en este se utiliza una ventana de $t_w = 3ns$ y la resolución de trabajo de $t_r = 1ns$.

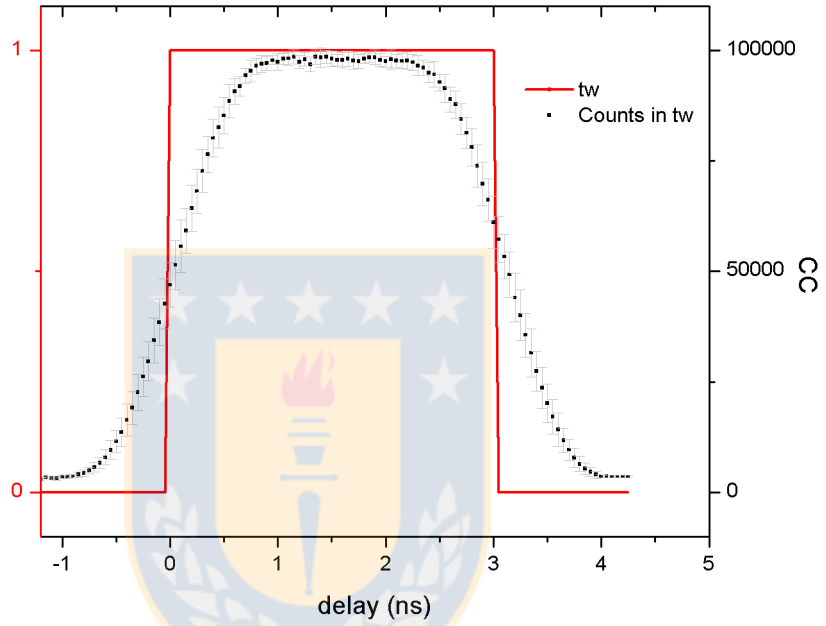


Figura 4.3: Cuentas coincidentes experimentales en una ventana tw. Utilizando un generador de delay, se realiza un barrido de retrasos entre dos señales provenientes de dos APDs. La primera señal abre una ventana de coincidencia, mientras que la segunda se retrasa con respecto a la primera, obteniendo cuentas coincidentes dentro de la ventana de detección.

El resultado en cuentas coincidentes mostrado en la figura 4.3, lo podemos modelar como la convolución entre $h(t_d)$ y la gaussiana $g(t_d)$, esto es:

$$(h * g)(t_d) = \int_{-\infty}^{\infty} h(\tau) \cdot g(t_d - \tau) d\tau, \tag{4.4}$$

$$= \int_{0}^{t_w} g(t_d - \tau) d\tau. \tag{4.5}$$

Asumiendo que nuestro modelo teórico es ideal en los límites impuestos y utilizando (4.2), obtenemos la diferencial de (4.4) como:

$$(g * h)' = N\mathrm{e}^{-\frac{(t_d-\mu)^2}{2\sigma^2}} - N\mathrm{e}^{-\frac{(t_d-t_w-\mu)^2}{2\sigma^2}} \tag{4.6}$$

La figura 4.4, muestra la diferencial experimental de una ventana de $t_w = 3ns$, evaluada con resoluciones de trabajo t_r de $1ns$ y $500ps$.

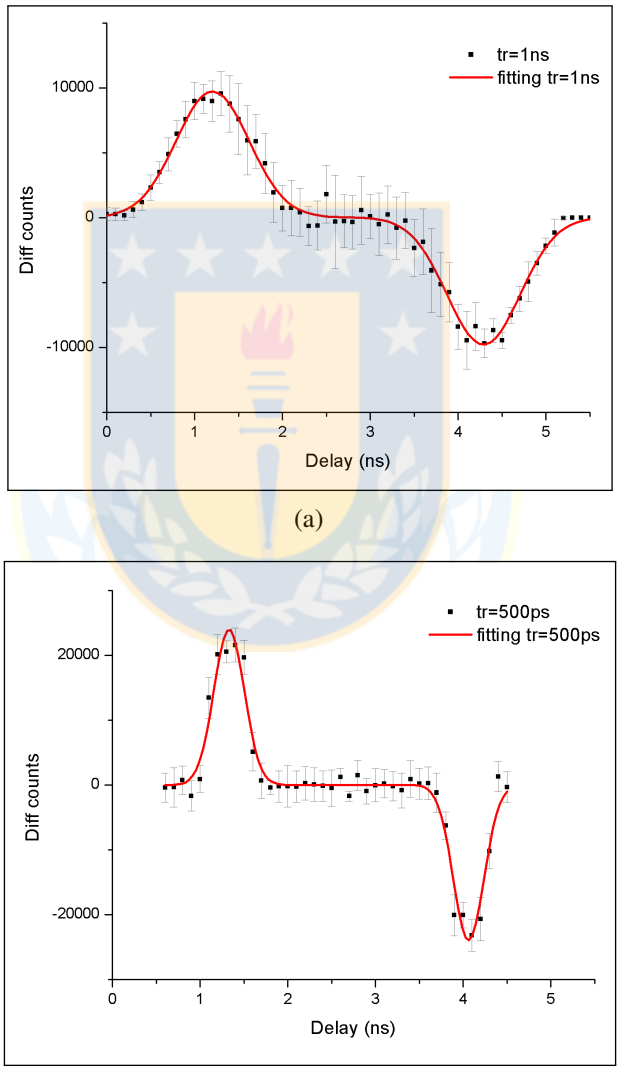


Figura 4.4: Fitting experimental utilizando una ventana de detección en coincidencia de $t_w = 3ns$. a) Resultados a resolución $t_r = 1ns$. b) Resultados utilizando $t_r = 500ps$.

Utilizando la ecuación 4.6 sobre múltiples ventanas t_w (con $t_r = 500ps$), se obtienen los valores mostrados en la tabla 4.1, donde la desviación estándar experimental del error electrónico obtenido fue de $\sigma = 0{,}173 \pm 0{,}00169ns$. Por otro lado, considerando la ecuación 4.1 sobre las mediciones experimentales de t_w, podemos obtener los parámetros de operación t_r y d_w del CCU. Luego, el sistema fue diseñado para operar a $t_r = 500ps$, sin embargo los resultados experimentales indican que se trabaja con resolución $t_r = 0{,}455 \pm 0,009ns$ y $d_w = 0{,}077ns$.

n	nt_r (ns)	σ (ns)		Experimental t_w (ns)		R^2
		mean	error	mean	error	
1	0.5	0.17568	0.032	0.460	0.080	0.900
2	1.0	0.17517	0.010	0.956	0.019	0.943
3	1.5	0.17152	0.009	1.407	0.018	0.949
4	2.0	0.17192	0.009	1.878	0.019	0.945
5	2.5	0.17303	0.009	2.357	0.019	0.943
6	3.0	0.17314	0.007	2.720	0.016	0.962

Tabla 4.1: Evaluación del error electrónico y t_w utilizando 500ps.

En base al análisis anterior se mide la resolución t_r y el ruido electrónico experimental, para otras resoluciones de trabajo sobre nuestro CCU, la cuales fueron estimadas por software (EDA). Estos resultados se muestran en la tabla 4.2, en ésta se aprecia como las resoluciones experimentales varían con las resoluciones de diseño.

Resolution time (ns)			σ	
For EDA	Experimental		(ns)	
	mean	error	mean	error
0.50	0.455	0.009	0.173	0.00169
1.00	1.008	0.073	0.293	0.00786
2.00	2.098	0.267	0.544	0.01600

Tabla 4.2: Estadística del error electrónico de una unidad CCU, para distintas resoluciones t_r.

Los resultados en la tabla 4.2, además indican que al mejorar la resolución de trabajo, no sólo se reducen las cuentas accidentales por el ancho de t_w, sino que en base a nuestro diseño también se reduce el error electrónico dentro del CCU. Finalmente, al considerar que la visibilidad óptica se ve afectada por el error electrónico del instrumento contador de coincidencia y el tamaño de la ventana de coincidencias, nuestro diseño disminuiría este ruido utilizando electrónica de bajo costo, con ello mejoraría los valores de visibilidad habilitando sistemas para información cuántica.

CAPÍTULO 5

AUMENTO DE VISIBILIDAD ÓPTICA EN CONFIGURACIONES CON ENTRELAZAMIENTO CUÁNTICO

Capítulo 5

Aumento de visibilidad óptica en configuraciones con entrelazamiento cuántico

En este capítulo se evalúan sistemas con fotones entrelazados, donde a través de técnicas de control y diseño avanzado en electrónica embebida se habilitan sistemas con entrelazamiento energía-tiempo, para enlaces de larga distancia con fibra óptica en laboratorio e instalada en terreno. Se finaliza el capítulo mostrando resultados en experimentos de sistemas de tres bases de medición, evaluando entrelazamiento con desigualdades generalizadas de CHSH.

5.1. Entrelazamiento energía-tiempo

Cuando dos partículas son generadas al mismo tiempo por un proceso de conservación de energía, y cuya dirección de propagación es completamente indeterminada, las partículas exhiben entrelazamiento energía-tiempo [17]. La configuración más utilizada para generar este tipo de entrelazamiento es utilizando un interferómetro de Franson [18], el cual se muestra en la figura 5.1.

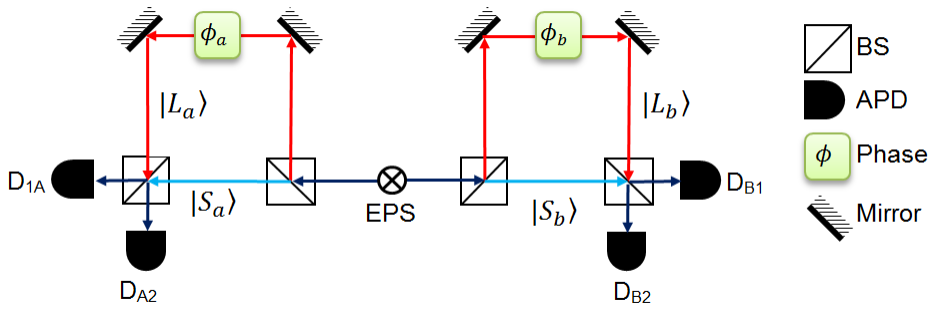


Figura 5.1: Esquema de Franson, para entrelazamiento energía-tiempo. La fuente EPS genera pares de fotones los cuales se inyectan en interferómetros des-balanceados, cuyas fases son: ϕ_a en Alice y ϕ_b en Bob.

En esta configuración, dos fotones simultáneamente emitidos son inyectados dentro de dos interferómetros de Mach-Zehnder desbalanceados (UMZ) [63, 64], donde la incertidumbre en el tiempo de emisión hace indistinguible la elección de camino que cada fotón pueda tomar. Según la figura 5.1, la fuente EPS genera pares de fotones los cuales son enviados en sentido contrario. En Alice, el fotón por incertidumbre puede tomar el camino largo $e^{\varphi_a}|L_a\rangle$ o el camino corto $|S_a\rangle$, donde φ_a es una fase propia de los UMZ, la cual puede ser controlada externamente. Al igual que en Alice, en Bob los caminos a tomar serán: $e^{\varphi_b}|L_b\rangle$ para el largo y $|S_b\rangle$ para el corto.

Bajo las condiciones anteriores, el estado conjunto del sistema queda como:

$$\begin{aligned} |\psi\rangle &= c_1\left(|S_a\rangle + e^{\phi_a}|L_a\rangle\right) c_2\left(|S_b\rangle + e^{\phi_b}|L_b\rangle\right), \\ &= c_1c_2\left\{|S_a\rangle|S_b\rangle + e^{\phi_a+\phi_b}|L_a\rangle|L_b\rangle + e^{\phi_a}|S_a\rangle|L_b\rangle + e^{\phi_b}|L_b\rangle|S_a\rangle\right\}, \end{aligned} \tag{5.1}$$

donde c_1 y c_2 son variables complejas. En el resultado de la ecuación 5.1 se presentan cuatro posibles eventos en coincidencia $|S_aS_a\rangle$, $|S_aL_b\rangle$, $|L_bS_a\rangle$ y $|L_aL_b\rangle$. Por su geometría, las coincidencias $|S_aL_b\rangle$ y $|L_bS_a\rangle$ se producirán con un retraso respecto a $|S_aS_a\rangle$ y $|L_aL_b\rangle$, y se pueden descartar ajustando la ventana de detección. En estas condiciones y optimizando la fuente, el estado entrelazado energía tiempo, estará descrito por:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|S_a\rangle|S_b\rangle + e^{(\phi_a+\phi_b)}|L_a\rangle|L_b\rangle\right]. \tag{5.2}$$

Aunque esta configuración fue ampliamente aceptada para generación de entrelazamiento energía-tiempo, la información descartada en las coincidencias $|S_aL_b\rangle$ y $|L_bS_a\rangle$, producen un loophole geométrico denominado post-selección [19]. Aunque se proponen variaciones en el esquema para cerrar este loophole, Cabello propone un cambio geométrico en base a UMZs en configuración “hug”. La figura 5.2 muestra dicha configuración, en ésta las coincidencias $|S_aL_b\rangle$ y $|L_bS_a\rangle$ no existen, logrando cerrar dicho loophole [17].

La violación de la desigualdad de CHSH utilizando esta configuración, fue demostrada por Lima sobre una mesa óptica en 2010 [20].

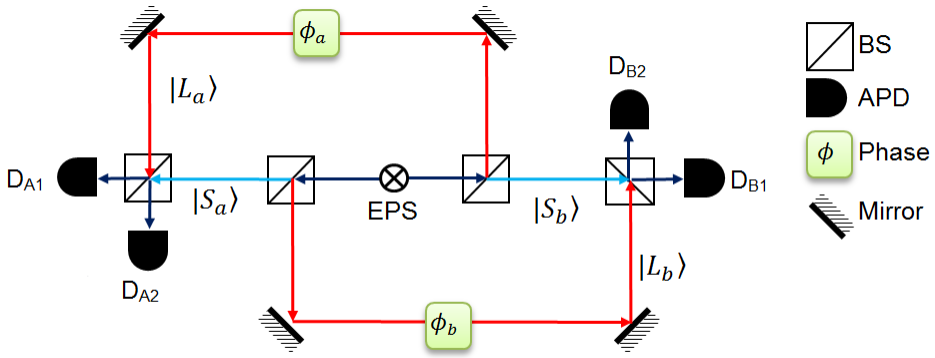


Figura 5.2: Interferómetro en configuración hug, para entrelazamiento energía-tiempo. La fuente EPS genera pares de fotones los cuales utilizando divisores de haz entran a dos brazos des-balanceados, con fases ϕ_a y ϕ_b.

En este esquema la desigualdad tiene la forma:

$$S = E(\phi_a, \phi_b) + E(\phi'_a, \phi_b) + E(\phi_a, \phi'_b) - E(\phi'_a, \phi'_b) \leq 2, \tag{5.3}$$

donde ϕ_a,ϕ'_a, ϕ_b y ϕ'_b son las bases a medir. El valor esperado está dado por $E(\phi_a, \phi_b) \equiv P_{11}(\phi_a, \phi_b)+P_{22}(\phi_a, \phi_b)-P_{12}(\phi_a, \phi_b)-P_{21}(\phi_a, \phi_b)$, donde $P_{ij}(\phi_a, \phi_b)$ es la probabilidad de detección en coincidencia entre los detectores D_{iA} y D_{jB} en Alice y Bob respectivamente. Esta probabilidad tiene la forma:

$$P_{ij}(\phi_a, \phi_b) = (1 - (-1)^{\delta_{ij}} V_{ij} cos(\phi_a + \phi_b)), \tag{5.4}$$

con

$$V_{ij} = \frac{C_{max} - C_{min}}{C_{max} + C_{min}}, \tag{5.5}$$

donde V_{ij} es la visibilidad de interferencia entre los detectores D_{iA} y D_{jB} en Alice y Bob, dada por los ángulos ϕ_a y ϕ_b. C_{max} y C_{min} representa las cuentas máximas y mínimas de interferencia en esa configuración.

Como las cuentas C_{min} están afectadas por el ruido del sistema, entonces la visibilidad es inversamente proporcional a dicho ruido. Con esto al disminuir el ruido del sistema, se maximiza la visibilidad.

Utilizando visibilidad máxima en (5.4) aplicado a (5.3), se obtiene:

$$S = cos(\phi_a + \phi_b) + cos(\phi'_a + \phi_b) + cos(\phi_a + \phi'_b) - cos(\phi'_a + \phi'_b). \tag{5.6}$$

Utilizando los desfases $\phi_a = -\frac{\pi}{4}$, $\phi'_a = \frac{\pi}{4}$, $\phi_b = 0$ y $\phi'_b = \frac{\pi}{2}$ en (5.6), se obtiene:

$$S = cos(-\frac{\pi}{4}) + cos(\frac{\pi}{4}) + cos(\frac{\pi}{4}) - cos(\frac{3\pi}{4}) = \frac{4\sqrt{2}}{2} = 2\sqrt{2}. \tag{5.7}$$

Como se aprecia en la ecuación 5.4, la certificación de entrelazamiento utilizando la desigualdad de CHSH depende de la visibilidad óptica y la estabilidad de las fases a medir. Aunque Lima logra violar la desigualdad obteniendo $S_{exp} = 2{,}54 \pm 0{,}04$ cerrando el loophole geométrico, este experimento no cierra el loophole de localidad, el cual se puede cerrar utilizado enlaces de larga distancia. La propuesta de nuestro grupo de trabajo es la utilización de fibra óptica para un sistema energía-tiempo, con el cual se cierra el loophole de localidad, y habilita un enlace que puede ser utilizado en QKD con el protocolo Ekert91. Sin embargo, este tipo de enlace presenta problemas por: dispersión, variación de fase, atenuación, entre otros.

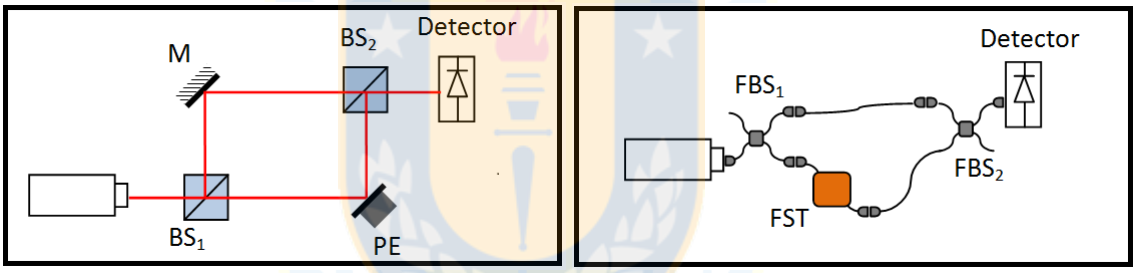
Como se aprecia en la ecuación 5.2, es fundamental que la fase entre las partículas entrelazadas sea fija para mantener un sistema con entrelazamiento. Por otro lado, la atenuación producida por la fibra óptica, implica una disminución de las cuentas entrelazadas disminuyendo el parámetro señal a ruido, y según las ecuaciones 5.4 y 5.5 produce una disminución de la visibilidad de interferencia, afectando dramáticamente la evaluación de la desigualdad de CHSH. Es por esto que tras el control de fase en el enlace cuántico, y la disminución del ruido electrónico sobre la ventana de coincidencia en la unidad contadora de coincidencia, en este trabajo buscamos el aumento de la visibilidad de interferencia, y con ello lograr la violación de las desigualdades de CHSH, habilitando enlaces de larga distancia utilizando fibra óptica con entrelazamiento energía-tiempo.

5.2. Control de fase en interferómetro de Mach-Zehnder

La división de un haz de luz coherente cuyas partes toman caminos diferentes para luego ser recombinadas utilizando elementos separados, es la base de un interferómetro de Mach-Zehnder (MZI) [63, 64]. La diferencia de camino (h) en el interferómetro, produce un desfase dado por:

$$\delta = \frac{2\pi}{\lambda_0} nh, \tag{5.8}$$

donde n es el índice de refracción. Por tanto, la fase δ es controlable a través de dicha diferencia de caminos [21]. Para esto, en espacio libre se puede utilizar un piezoeléctrico sobre un espejo (figura 5.3.a) , y en fibra óptica un estirador de fibra basado en un elemento piezo eléctrico, al cual llamaremos "stretcher" de fibra (figura 5.3.b).



(a) (b)

Figura 5.3: MZI como controlador de fase. a) Sistema básico, utiliza un espejo (M) dos divisores de Haz (BS) y un piezoeléctrico (PE). b) Sistema en fibra óptica, este esquema utiliza dos divisores de haz para fibra (FBS) y un stretcher de fibra (FST).

En ambos esquemas se utiliza un dispositivo activo, el cual es capaz de variar la dimensión de uno de los caminos en función de un voltaje aplicado ($h \propto V$). Con esto, la ecuación que regirá la fase estará dado por:

$$\delta(V) \propto \frac{2\pi}{\lambda_0} nV. \tag{5.9}$$

La figura 5.4 muestra mediciones experimentales a la salida de un MZI montado en laboratorio, en ésta se aprecia como la potencia RMS en el detector tiene una tendencia dada por (ver Apéndice E):

$$P \propto cos(\frac{\delta(V)}{2})^2 = \frac{1}{2}(1 + cos(\delta(V)). \tag{5.10}$$

El actuador para esta prueba fue un piezoeléctrico (figura 5.3.a), la señal de excitación utilizada fue una rampa entre $0V < V(t) < 50V$, pero sólo se gráfica la región entre $8V < V(t) < 16V$. Como se aprecia, si el control opera en la región $-\pi < \delta < 0$, entonces el sistema se comportaría como un sistema lineal de segundo orden. Con esta base es posible proponer la implementación de un control proporcional integral derivativo clásico (PID), que permita mantener la fase controlada.

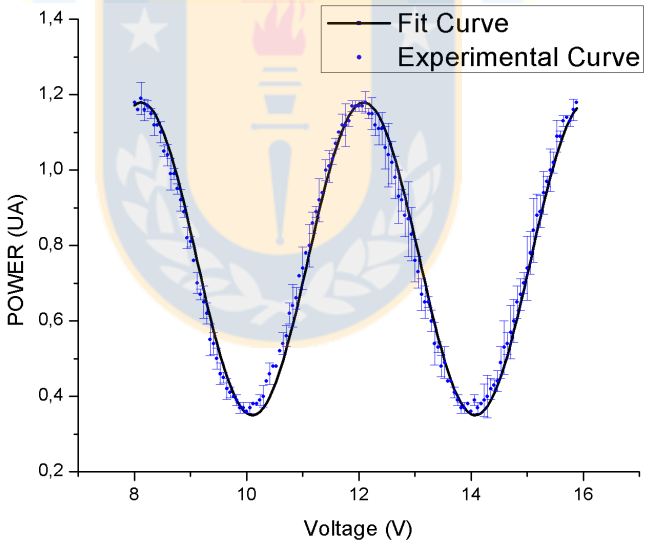


Figura 5.4: Medición de potencia experimental (en unidades arbitrarias), de interferómetro MZI armado en mesa óptica.

5.3. Control proporcional integral derivativo

Considerando el sistema realimentado que se muestra en la figura 5.5, el control ($u_c[k]$) será la entrada de una planta $y[t] = \frac{1}{2}(1 + cos(\varphi_0 + \varphi[k] + u_c[k])$, donde φ_0 y $\varphi[k]$ son la fase inicial y el ruido en función del tiempo respectivamente. La entrada al controlador es el error del sistema ($e[k]$), donde éste es la diferencia entre la salida y una señal de referencia ($e[k] = y[k] - ref$).

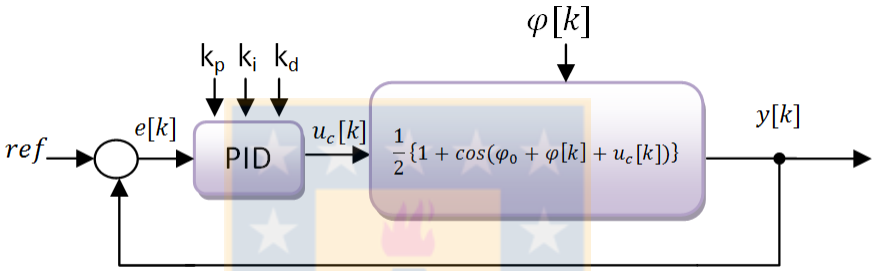


Figura 5.5: Diagrama de bloque del sistema modelado.

El control PID en el plano de *Laplace*, esta dado por:

$$U(s) = K\left[1 + \frac{1}{sT_i} + sT_D\right]E(s). \tag{5.11}$$

Aunque existen diversas formas de aproximación numérica para discretizar una ecuación en Laplace [65], en este trabajo utilizamos la aproximación de *Euler-Forward*, para integrar este control a un sistema embebido, la cual está dada por: $\frac{1}{s} = \frac{z-1}{zT}$. Luego, aplicando esta transformación sobre (5.11), se obtiene:

$$\begin{aligned} u_{cF}[k] = u_{cF}[k-1] + K_p\left\{y[k-1] - y[k]\right\} + k_d\left\{ref - y[k]\right\}, \\ + k_i\left\{2y[k-1] - y[k-2] - y[k]\right\}. \end{aligned} \tag{5.12}$$

Cabe señalar que no es posible utilizar la sintonización del controlador, debido a que el sistema no es lineal. Sin embargo, el ajuste de los parámetros de control pueden realizarse en la marcha, ya que una vez encontrada la región lineal, el PID podría trabajar normalmente.

5.4. Control de fase en entrelazamiento energía tiempo

La ecuación de control obtenida será aplicada a una configuración hug sobre $1km$ de fibra óptica en laboratorio. La configuración experimental se muestra en la figura 5.6, esta configuración contempla cuatro partes; fuente, línea de retraso, detecciones en Alice y detecciones en Bob.

La fuente de emisión contempla la unión de un láser de bombeo ($405nm$) y uno de control ($852nm$), los que inciden sobre un cristal PPKTP para 405nm con generación ortogonal (tipo II) [61]. Por sus propiedades, el cristal PPKTP generará pares de fotones a $810nm$ (del haz de $405nm$), mientras que la señal de control se mantendrá en $852nm$. Los pares de fotones son separados por un divisor de haz en polarización (PBS_1), y entran al interferómetro Hug en BS_1 y BS_2 respectivamente. Aunque los brazos tienen largos distintos, la diferencia entre ellos es sólo $2m$.

La fuente y Alice se encuentran en el mismo laboratorio, mientras que Bob estará separado por $1km$ de fibra óptica. Finalmente, la línea de retraso compensará la diferencia entre los brazos S_b y L_b, de tal forma de obtener $S_b - L_b = S_a - L_a$, y con ello encontrar la zona de entrelazamiento. Cabe señalar, que la señal de control es un haz continuo, que al pasar por el PBS_1 y los BSs siguientes sólo se dividirá en partes iguales, permitiendo sensar y controlar la fase en los interferómetros L_a-S_a y L_b-S_b por separado.

En la figura 5.6, podemos ver dos interferómetros UMZ. El primero es formado por los brazos L_a-S_a, cuya fase será controlada utilizando un piezo-eléctrico. Los haces se separan utilizando un filtro (F_2 de $810 \pm 1nm$) sobre las salidas de FBS_1, permitiendo el paso de los fotones entrelazados y desviando el haz de control. La señal de control es sensada utilizando un diodo p-i-n (Pin_1), realimentado el algoritmo PID sobre el $FPGA_1$.

El segundo interferómetro a controlar es L_b-S_b, el cual esta diseñado completamente en fibra óptica. Por esto, el actuador será un stretcher de Fibra, el cual es controlado por el algoritmo PID en la $FPGA_2$. La lectura de control se obtiene el FBS_2 de forma similar al anterior.

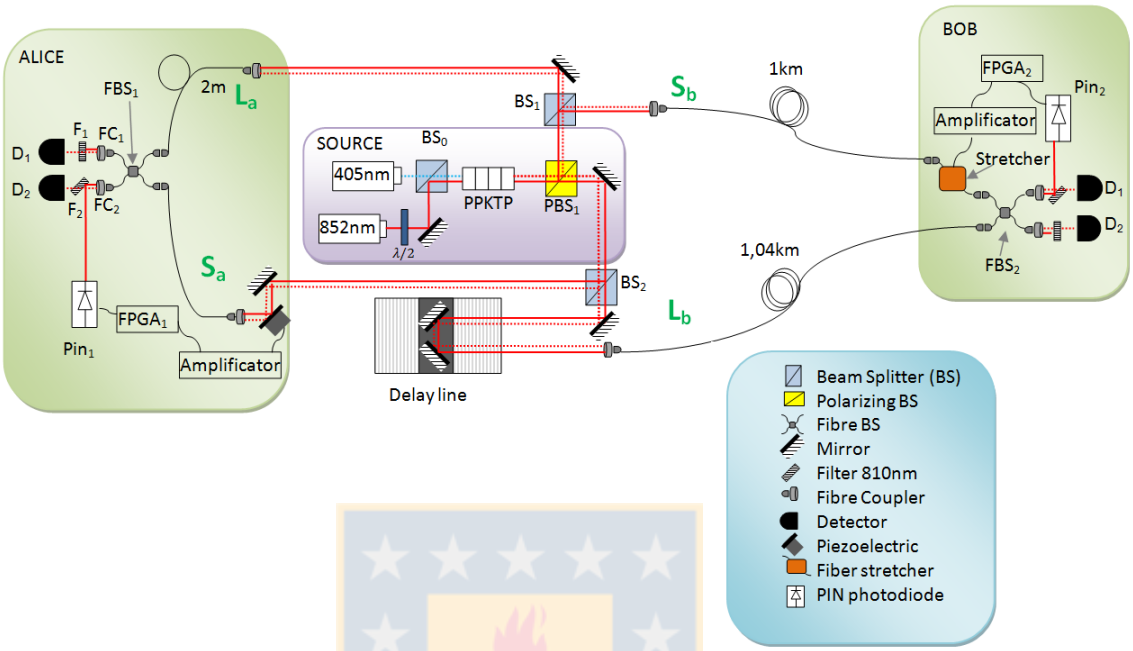


Figura 5.6: Configuración experimental para evaluación de entrelazamiento energía tiempo. La fuente genera pares entrelazados a través de un cristal PPKTP, dichos fotones son combinados con un láser de control utilizando un divisor de Haz (BS). Ambas señales son enviadas a Alice y Bob utilizando un enlace en espacio libre para Alice y en fibra óptica para Bob. El láser de control es medido utilizando diodos p-i-n, cuyas salida es conectada a un controlador PID en base a un FPGA, estabilizando la fase por brazo en cada estación. Con la fase controlada, los fotones entrelazados son detectados al final de cada estación, utilizando detectores APD. Finalmente, con estas mediciones se puede evaluar la desigualdad de CHSH

La figura 5.7 muestra los resultados experimentales del control de fase, en la configuración hug de $1km$. En ésta, se evalúa que la fase siga una referencia triangular (entre $0s - 5,5s$), mientras que en el tiempo posterior se cancela el control y se ingresa una señal triangular en el actuador, para obtener los máximos y mínimos de fase para el sistema experimental.

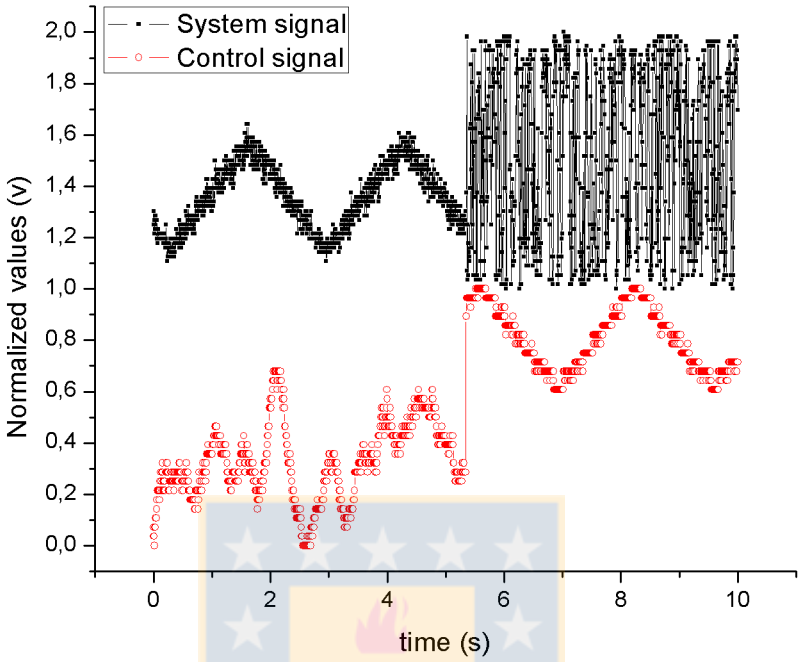
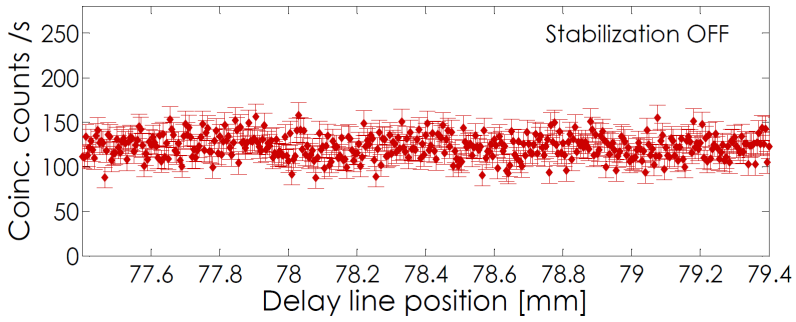


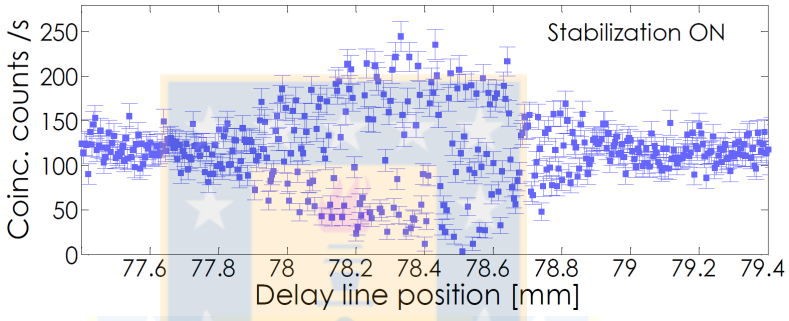
Figura 5.7: Resultados obtenidos del control sobre el sistema montado en el laboratorio.

5.5. Resultados preliminares en entrelazamiento energía tiempo

Experimentalmente, el estado $|\psi\rangle = \frac{1}{\sqrt{2}}\left[|S\rangle\,|S\rangle + e^{(\phi_a-\phi_b)}\,|L\rangle\,|L\rangle\right]$ sólo se genera en la región simétrica ($L_A - S_A = L_B - S_B$). Para visualizar este estado se varia la fase ϕ_A cíclica y controladamente, logrando apreciar una interferencia en las lecturas de cuentas en coincidencias. Sin embargo, la interferencia sólo se apreciará cuando ϕ_B permanezca fija, y a medida de que la línea de retraso se acerque a la región simétrica. La figura 5.8.a muestra los resultados al analizar la región simétrica, con el control de fase sobre ϕ_B apagado. Como es de esperar, la interferencia no existe debido a que las fases ϕ_A y ϕ_B son variables, producto de ruido dentro del interferómetro. Al activar el control de fase sobre ϕ_B, y nuevamente revisar la región de simetría, se observa el patrón mostrado en la figura 5.8.b.



(a)



(b)

Figura 5.8: Detecciones en coincidencias sobre la región simétrica. a) Patrón de interferencia con estabilización de fase inactiva. b) Patrón de interferencia con estabilización de fase activa sobre ϕ_B.

Con el patrón de interferencia encontrado es posible evaluar la conexión cuántica, utilizando las ecuaciones de Lima [20]. Los resultados obtenidos para todas las combinaciones de probabilidad $P_{ij}(\phi_A, \phi_B)$, se muestran en la figura 5.9. Considerando D_{A1}, D_{A2}, D_{B1} y D_{B2} como los pares de detectores en Alice y Bob respectivamente. En base a estas mediciones, la desigualdad obtenida fue $S = 2{,}39 \pm 0{,}12$, que implica una violación mayor a $3{,}25$ desviaciones estándar. Este resultado es la primera demostración experimental, de una violación de la desigualdad de CHSH, utilizando entrelazamiento energía tiempo, en una configuración sin loophole geométrico, sobre un enlace de fibra óptica de $1km$ de largo. Produciendo un importante avance para seguridad en comunicación cuántica de larga distancia, utilizando fibra óptica [66].

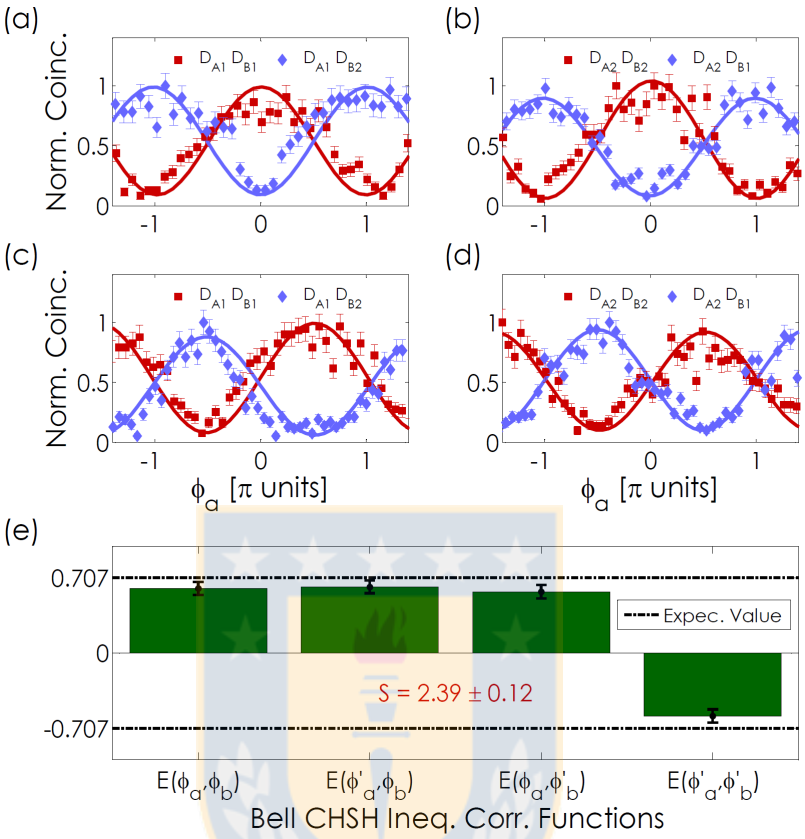


Figura 5.9: Curvas de interferencia y violación de las desigualdades CHSH. Graficos (a)-(d) muestran coincidencia normalizadas de las detecciones en Alice y Bob. (a) y (b) corresponden a los casos donde $\phi_b = 0$ y (c) y (d) a los de $\phi_b = \pi/2$. e) muestra los valores de probabilidad para cada función de correlación (E), aplicadas en el test de CHSH, con las cuales se obtiene $S = 2{,}39 \pm 0{,}12$.

5.6. Caracterización de variación de fase en interferómetro de fibra montado en terreno

El segundo hito de este trabajo es implementar la configuración hug bajo una conexión de larga distancia, y bajo condiciones ambientales externas.

Para esto, se cuenta con un enlace de fibra óptica de $1500nm$ y $3{,}7km$ de largo, la cual está instalada en la Universidad de Concepción, entre el edificio de Ingeniería Eléctrica e instalaciones externas. El diagrama de la configuración hug y las instalaciones utilizadas se muestran en la figura 5.10, en esta imagen se agrega un plano con la separación y elevación espacial entre las ubicaciones de Alice y Bob.

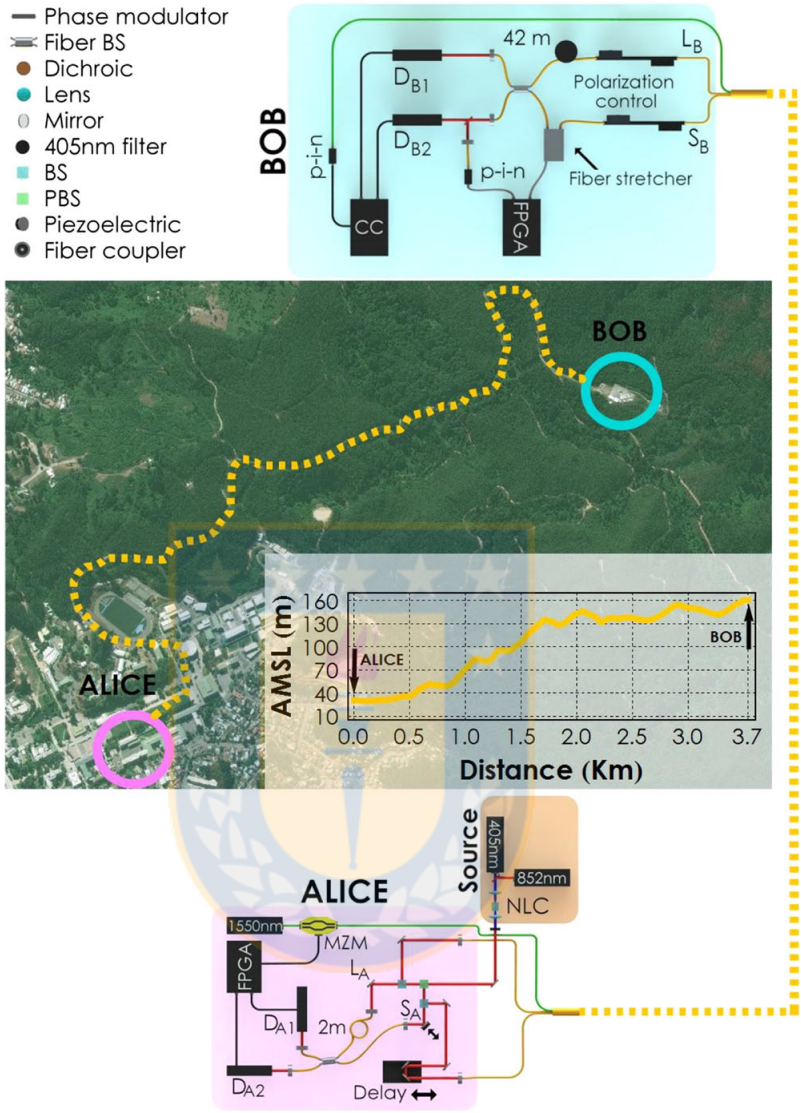


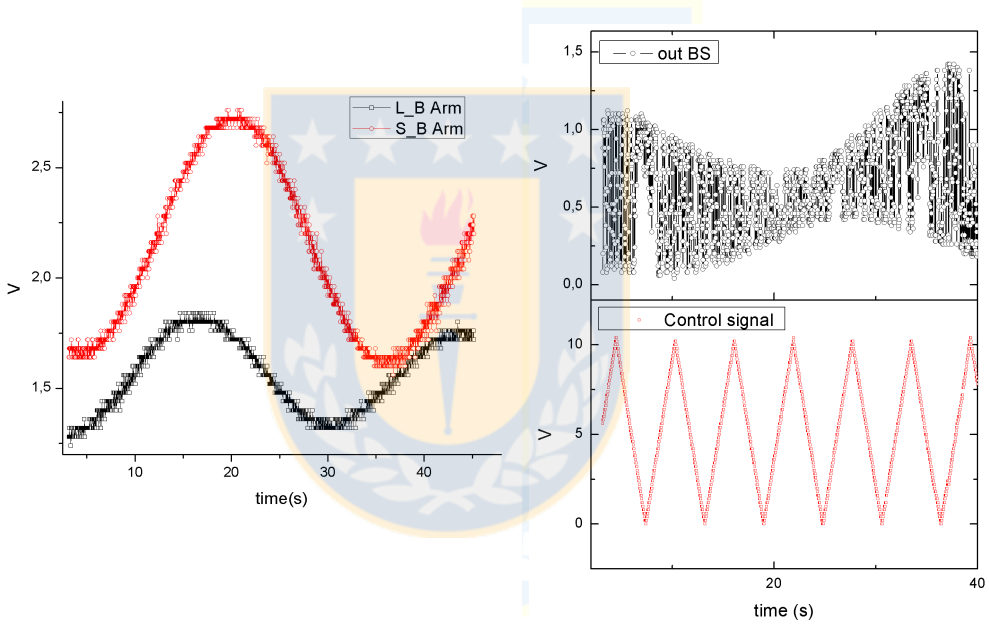
Figura 5.10: Configuración experimental para evaluación de entrelazamiento energía tiempo con fibras instaladas en terreno.

Aparte del emplazamiento, otra de las diferencias notorias entre la configuración actual y la anterior, son la inclusión de un dispositivo generador de pulsos en Alice. Este dispositivo permitirá evaluar las cuentas en coincidencias en la posición de Bob, y su función es repetir los pulsos de detección en D_{A1}, esto pulsos son evaluados en tiempo real con las detecciones retrasadas en el contador de Bob.

Luego de instalar el esquema y realizar las primeras pruebas, se observa que la pérdida de fotones en canal cuántico es crítica. Ejemplo de esto es que al generar 270000 ± 24000

pares de fotones sólo 9000 ± 130 llegan a Bob ($3\,\%$), con estas cuentas se obtienen solamente 35 ± 6 cuentas coincidentes (en la región de coincidencia). Considerando una ventana de $2ns$ se estima que las cuentas accidentales son $5{,}3 \pm 0{,}7$ cuentas, lo que implica que un $14\,\%$ de las cuentas en coincidencia son ruidos no deseados.

Otro de los problemas presentes en esta configuración es que el interferómetro L_B-S_B (ver figura 5.10), presenta variaciones de intensidad en cada brazo bajo una emisión de luz constante, fenómeno mostrado en la figura 5.11.a.



(a) (b)

Figura 5.11: Detección de señal de control sobre el foto-detector p-i-n fibra montada en terreno. a)Intensidad por brazo, señal de control constante. b) Intensidad en la salida del BS de Bob, señal de control variable.

Por otro lado, en la figura 5.11.b se muestra la respuesta del interferómetro a una señal triangular sobre el stretcher de fibra, como se aprecia la respuesta es una señal variable en el tiempo, cuyo modelo es de la forma (ver Apéndice F):

$$P \propto c(t)cos(\frac{\delta(V)}{2})^2 + b(t) \equiv \frac{c[k]}{2}\,(1 + cos(\delta_0 + \delta[k])) + b[k]. \tag{5.13}$$

5.7. Estabilización de fase para interferómetro de fibra instalada en terreno

Utilizando la expresión de la ecuación 5.13, el sistema a controlar queda definido por el diagrama de la figura 5.12. En este sistema el problema de control ya no es trivial, ya que las perturbaciones en cada brazo producen un sistema no lineal y multi-variable.

En el sistema inicial las intensidades por brazo eran idénticas y fijas, lo que implica que la modulación o control de fase se restringía en un rango fijo. Con esto, el controlador podía seguir cualquier referencia dentro de este rango de trabajo.

Para el sistema actual, dicho rango es variable en el tiempo producto del factor $c(t)$, lo que implica que la referencia tiene limites variables, haciendo imposible seguirla si ésta es fija en el tiempo, más aún si lográsemos identificar el rango de trabajo el factor aditivo $b(t)$ nos podría alejar de dicha región, esforzando innecesariamente el actuador (piezoeléctrico o stretcher).

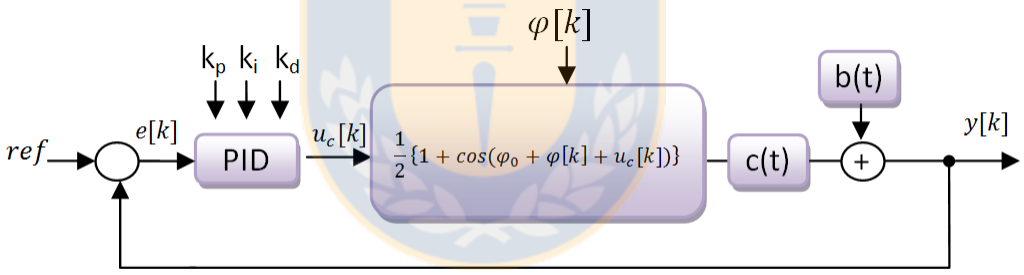


Figura 5.12: Diagrama de bloques, nuevo modelo de sistema con perturbaciones por brazos.

Por estos motivos el controlador a diseñar se restringe a mantener una fase estable, y no establecer una como el sistema anterior (ver figura5.7). Con lo expuesto, la estabilización de fase debe ser en el centro de la función $c(t)$ y así lograr permanecer en la región de trabajo. Una forma sencilla de generar esta condición es eliminado el offset $b(t)$, utilizando un filtro pasa alto después del foto-detector.

La figura 5.14.a muestra la estabilización de fase utilizando un filtro pasa bajo y $ref = 0$. Aunque el diseño estabiliza la fase, no aparece interferencia en la región de operación. La explicación de esto, es que el controlador PID actuando después de un filtro pasa altos, genera un control muy esforzado. Este defecto afecta directamente en la estabilización de fase, aumentando la variación por estimulación piezoeléctrica.

Con lo anterior, se hace necesario implementar un algoritmo dedicado, para esto evaluamos la planta modelada en (5.13), con la forma:

$$y[k] \equiv \frac{c[k]}{2}\left(1 + cos(\delta_0 + \delta[k] + u_c[k])\right) + b[k]. \tag{5.14}$$

Utilizando esta expresión, el error a controlar tendrá la forma:

$$\begin{aligned} e[k] &= ref - y[k-1], \\ &= (ref - b[k-1]) - \frac{c[k-1]}{2}\left(1 + cos(\delta_0 + \delta[k-1] + u_c[k-1])\right). \end{aligned} \tag{5.15}$$

Sí consideramos $ref = \hat{b} \approx b[k]$ sobre (5.15), entonces el error a minimizar estará dado por:

$$e[k] \approx -\frac{c[k-1]}{2}\left(1 + cos(\delta_0 + \delta[k-1] + u_c[k-1])\right) \tag{5.16}$$

Con lo expuesto en (5.16), el controlador actuaría directamente sobre la fase del sistema $\delta[k-1]$, independiente de la perturbación en amplitud $c[k]$. En este escenario se propone utilizar una media móvil para estimar $\hat{b}$, la cual será obtenida en intervalos de tiempo configurables.

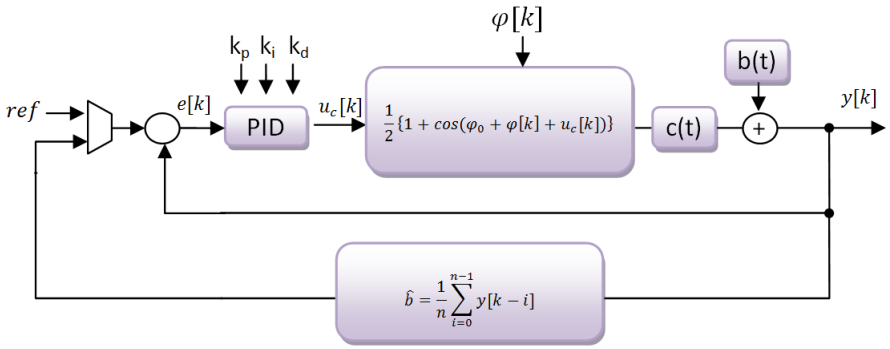


Figura 5.13: Diagrama de control con "media móvil" en interferómetro con perturbaciones por brazos.

Finalmente, en la figura 5.13 se muestra el nuevo diagrama de control a implementar sobre la FPGA. Como se aprecia, la "media móvil" es calculada directamente sobre la salida del sistema, lo que implica que si $b(t)$ varía pero esta dentro del rango de trabajo impuesto por $c(t)$, el valor de $\hat{b}$ se mantendrá constante, permitiendo que el controlador evite esfuerzos innecesarios.

La figura 5.14.b muestra los resultados experimentales de estabilización de fase, utilizando algoritmo con media móvil. Como se aprecia, una vez calculada la media ($\hat{b}_1$), ésta se mantendrá fija hasta que $b(t)$ y $c(t)$ cambien radicalmente sus estados, habilitando la obtención de una nueva media ($\hat{b}_2$) y con ello una nueva región de trabajo, donde el controlador opere con mínimo esfuerzo.

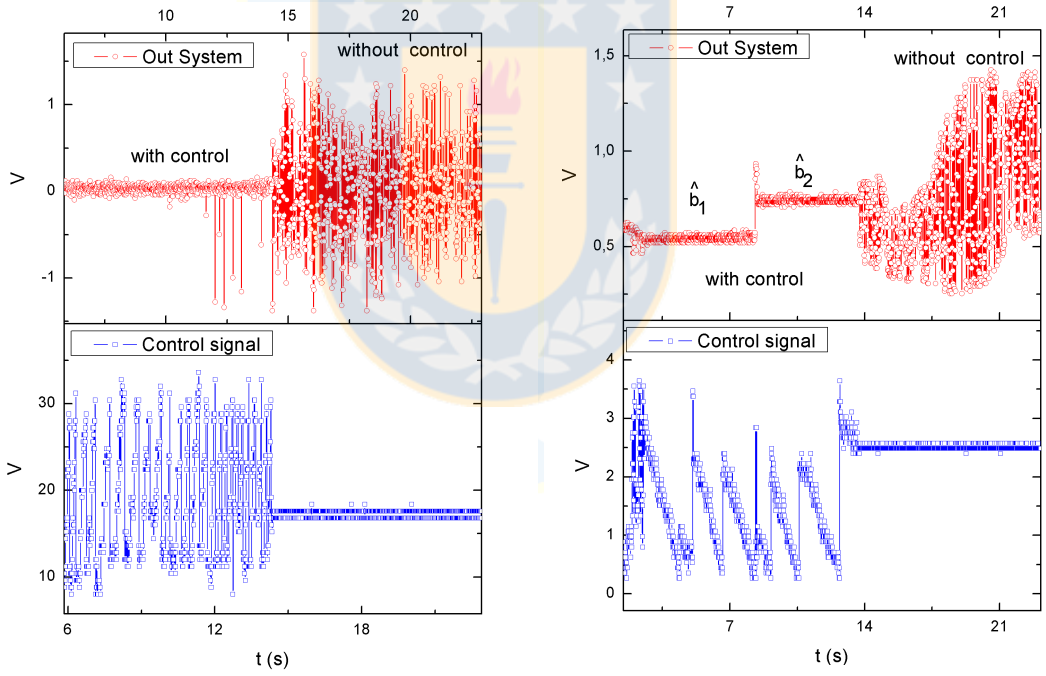
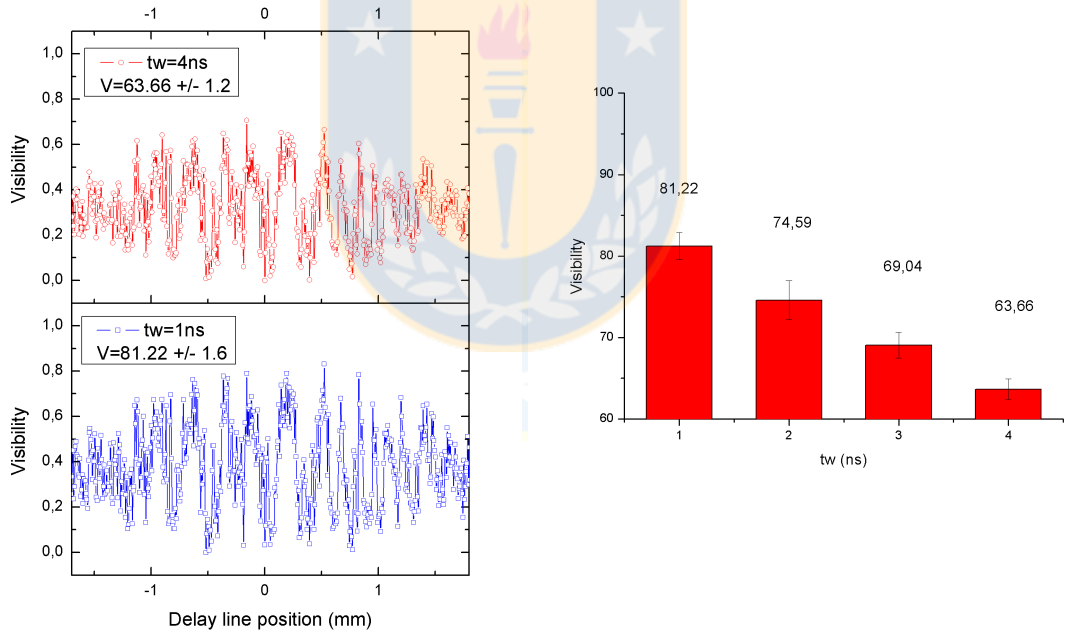


Figura 5.14: Estabilización de fase 3.7km de fibra instalada en terreno. a) Control por filtro pasa alto. b) Control utilizando algoritmo en base estimación de "media móvil"

5.8. Evaluación de enlace cuántico instalado en terreno

Considerando las condiciones en la sección 5.5, y utilizando el nuevo sistema de control, se obtiene la interferencia en la región de simetría. La forma de ésta se muestra en la figura 5.15.a, donde se utilizan ventanas de $tw = 4ns$ y $tw = 1ns$, obteniendo una visibilidad de $V = 63{,}66 \pm 1{,}25$ y $V = 81{,}22 \pm 1{,}65$ respectivamente. Cabe señalar, que el aumento de la visibilidad es producto de la filtración de cuentas accidentales (producto del tamaño de la ventana de detección), y de la disminución del error electrónico en el dispositivo contador de coincidencias, tal como se explica en las secciones anteriores. La figura 5.15.b, muestra como se maximiza la visibilidad disminuyendo la ventana de coincidencia (t_w).



(a) (b)

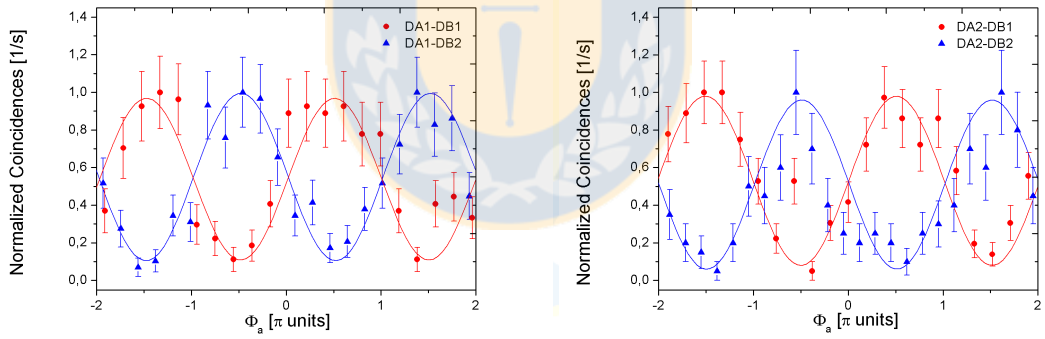
Figura 5.15: Visibilidad de estados cuánticos sobre enlace de 3.7km. a) Visualización de interferencia utilizando ventanas $t_w = 4ns$ y $t_w = 1ns$. b) Evaluación de visibilidad en función de t_w.

En base a la medición de interferencia utilizando una fase fija en Bob, y asumiendo simetría en el experimento [67], podemos evaluar la violación de CHSH como:

$$S = 3E(\phi_A, \phi_B) - E(\phi_A^{'}, \phi_B), \tag{5.17}$$

donde $E(\phi_A, \phi_B) = P_{11}(\phi_A, \phi_B) + P_{22}(\phi_A, \phi_B) - P_{12}(\phi_A, \phi_B) - P_{21}(\phi_A, \phi_B)$, con P_{ij} correspondiente a la probabilidad de detección en coincidencia en los detectores i y j de Alice y Bob, bajo ciertos ϕ_A y ϕ_B respectivamente. Mientras que las fases utilizadas para una máxima violación de CHSH, fueron: $\phi_A = \frac{\pi}{4}$, $\phi_A^{'} = -\frac{\pi}{4}$, $\phi_B^{'} = 0$.

Desde la data de la figura 5.16 calculamos el valor $S = 2{,}32 \pm 0{,}11$, violando la desigualdad de CHSH por sobre 2.94 desviaciones estándar, certificando por primera vez un enlace cuántico bajo la configuración hug, utilizado interferómetros de 3.7km de fibra óptica [68].



(a) (b)

Figura 5.16: Resultados experimentales para evaluación de la desigualdad CHSH. Medidas de cuentas en coincidencias normalizadas, entre los detectores DAi y DBi de Alice y Bob respectivamente.

5.9. Resultados experimentales evaluando Chained-Bell-Inequalities

Braunstein y Caves introdujeron una generalización a la desigualdad de Clauser-Horne-Shimony-Holt (CHSH), conocida como Chained-Bell inequalities [14]. Éstas son una familia de desigualdades en las cuales Alice y Bob pueden escoger entre $N \geq 2$ configuraciones de medidas, cada una con 2 posibles resultados (+1 y -1). Estas desigualdades tienen interesantes aplicaciones, entre las cuales destaca $n = 3$, donde se supera un loophole que ocurre en algunos experimentos basados en la desigualdad CHSH [15].

En nuestro experimento utilizamos una Chained-Bell Inequality usando $n = 3$, que en términos de probabilidades la escribimos como:

$$I_{chained} = p(a_0, b_0) - p(a_0, b_1) + p(a_1, b_1) - p(a_1, b_2) + p(a_2, b_2) - p(a_2, b_0) \leq 1, \quad (5.18)$$

donde $p(a_i, b_j)$ es la probabilidad de obtener el resultado -1, cuando Alice implementa la medida a_i y Bob b_j. La mecánica cuántica predice un valor máximo de $3\sqrt{3}/4 \approx 1{,}299$, cuando Alice y Bob comparten un estado máximamente entrelazado.

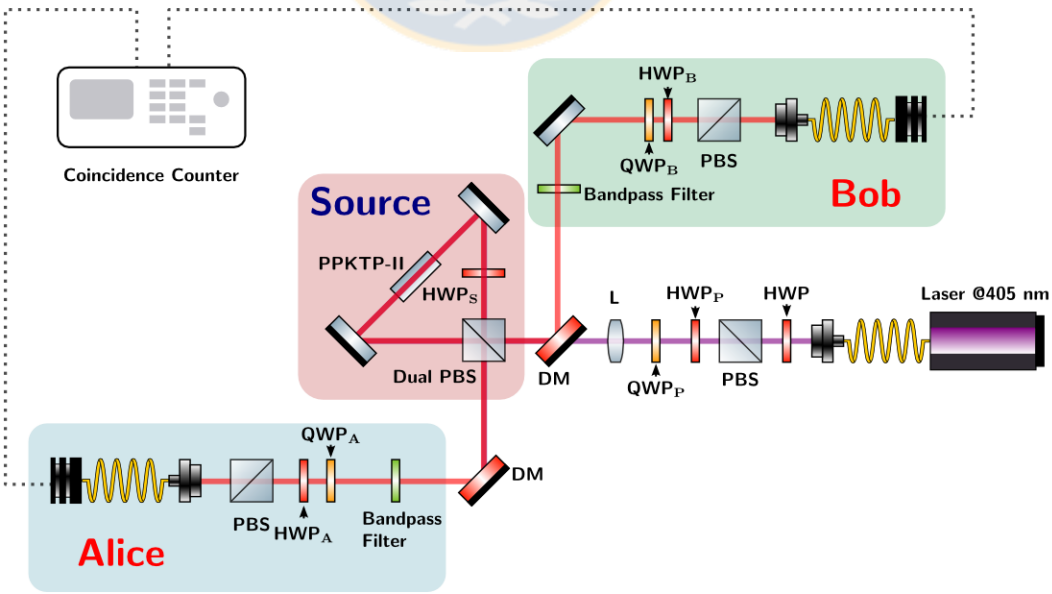


Figura 5.17: Configuración experimental para evaluación de desigualdad de $I_{chained}$.

La implementación del experimento se muestra en la figura 5.17, en éste usamos pares de fotones degenerados en 810 nm con polarizaciones ortogonales, producidos en la conversión paramétrica descendente (SPDC) usando un cristal PPKTP bulk tipo II de $2cm$ de largo [61]. El cristal es bombeado usando un láser monomodo contínuo emitido en 405 nm con 1 mW de potencia. Implementamos un interferómetro Sagnac, donde el cristal no lineal es colocado dentro de éste [69]. Este interferómetro está compuesto por dos espejos, una placa de media onda y un cubo divisor de haz por polarización. La placa de media onda está orientada en $45°$, permitiendo que a la salida del interferómetro el estado de los fotones generados sea:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle). \tag{5.19}$$

Para evitar entrelazamiento en otros grados de libertad, filtros de interferencia centrados en 810 nm (5 nm FWHM) fueron colocados, además de fibras monomodo para acoplar los fotones generados por la fuente.

Para implementar máxima violación de la desigualdad $I_{chained}$, se usaron placas de media onda y cubos divisores de haz por polarización en cada salida del interferómetro, para acoplar las fibras monomodo a los detectores.

Utilizando nuestro CCU diseñado, obtuvimos medidas para ventanas de coincidencia de 0.5ns, 1ns, 2ns y 4ns. La figura 5.18 muestra los resultados obtenidos de la mediciones descritas en (5.18). En ésta se aprecia como el aumento de resolución maximiza la visibilidad, y por ende habilita la violación de la desigualdad de $I_{chained}$ para $n = 3$ con mayor fidelidad.

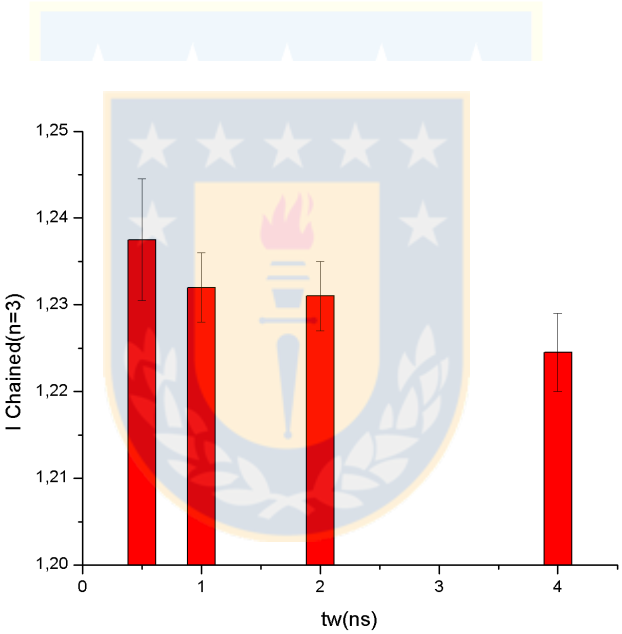


Figura 5.18: Violación experimental de la desigualdad de $I_{chained}$ utilizando $n = 3$.

CAPÍTULO 6

GENERACIÓN DE NÚMEROS ALEATORIOS PRIVADOS

Capítulo 6

Generación de números aleatorios privados

Los números aleatorios son esenciales para múltiples aplicaciones, como seguridad financiera, digital, comunicacional, etc. Una opción para generar éstos es la utilización de generadores cuánticos de números aleatorios (QRNG) [10], los cuales se basan en la incertidumbre de las mediciones cuánticas.

Sin embargo, si un agente externo altera este tipo de generador, de tal forma que las estaciones generen una trama aleatoria, pero conocida por el espía (la cual puede ser avalada por pruebas estándar de aleatoriedad [70]), la generación de números aleatorios no será privada.

Aunque la solución a este problema es la utilización de QRNGs independientes de los dispositivos [71], su implementación aún no es práctica.

Uno de los objetivos en esta tesis, es la implementación de un nuevo protocolo para generación privada de números aleatorios, el cual se basa en *semi-device-independent* (SID), propuesto por Pawlowski y Brunner [36]. La idea en SID, implica generación de números aleatorios en un sistema cuántico independiente de los dispositivos, cuya dimensión es conocida.

6.1. Sistema cuántico para generación de números aleatorios privados

El escenario de preparación y medición de estados cuánticos, con dimensión 2, se muestra en la figura 6.1. En este esquema, el emisor (Alice) prepara un qubit desconocido $|x\rangle$ utilizando un aparato P. Este estado es elegido según una entrada aleatoria x de dos bit ($x \in \{00, 01, 10, 11\}$), la cual es obtenida utilizando un QRNG comercial. En el receptor (Bob), dicho estado será medido utilizando un aparato M basado en una proyección $|m_z\rangle$, seleccionada con otra entrada aleatoria $z \in \{0, 1\}$, cuyo resultados será $b \in \{0, 1\}$.

La emisión podrá ser bloqueada por el aparato B, el cual será activado y desactivado por la entrada y. Este parámetro está condicionado a un tercer QRNG y una variable λ, la cual permite controlar la tasa de bloqueo. Cuando el bloqueo sea activado y/o producto de la baja eficiencia del detector, la salida en M será $\emptyset$, entonces el conjunto de salidas está dado por $b \in \{0, 1, \emptyset\}$.

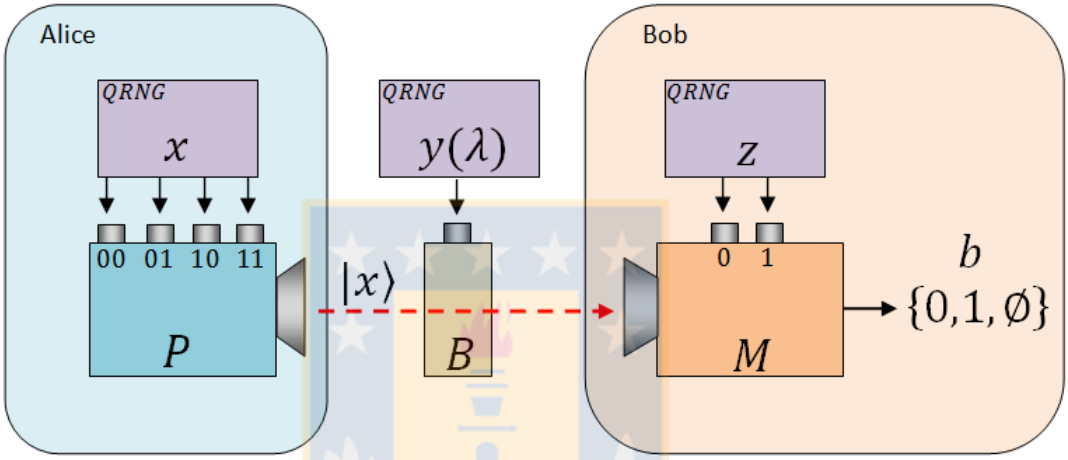


Figura 6.1: Escenario de preparación y medida de nuestro protocolo SDI para generación de números aleatorios privados.

6.1.1. Quantum random access code

La operación emisión-recepción propuesta puede ser vista como $2 \rightarrow 1$ random-access-code (RAC). En RACs Alice codifica m bits sobre un único bit, el cual envía a Bob, de tal forma que Bob pueda encontrar el valor de cualquiera de los m bits con probabilidad media de éxito p^c_{AV}.

De forma clásica, en una configuración $2 \rightarrow 1$, Alice puede enviar el primer bit con estado fijo y el segundo con estados aleatorios. Si Bob está interesado en el segundo bit, el tendrá una probabilidad media de adivinar el valor del segundo bit, dada por $p^c_{AV} = (\frac{1}{2} + \frac{1}{4}) = 0{,}75$ [72]. Sin embargo, la configuración SDI a implementar se basa en la utilización de Quantum-random-access-code (QRAC), donde m bits clásicos son codificados sobre unos pocos qubits, de tal forma que un arbitrario bit de los m codificados pueda ser recuperado utilizando mediciones cuánticas.

Un ejemplo de configuración QRAC, considera la preparación de $|x\rangle$, como:

$$\begin{aligned} |00\rangle &= cos(\pi/8)\,|0\rangle + sen(\pi/8)\,|1\rangle\,, \\ |01\rangle &= cos(7\pi/8)\,|0\rangle + sen(7\pi/8)\,|1\rangle\,, \\ |10\rangle &= cos(3\pi/8)\,|0\rangle + sen(3\pi/8)\,|1\rangle\,, \\ |11\rangle &= cos(5\pi/8)\,|0\rangle + sen(5\pi/8)\,|1\rangle\,, \end{aligned} \tag{6.1}$$

donde $|0\rangle$ y $|1\rangle$ son polarizaciones horizontal y vertical del fotón. Luego, Bob medirá dichos estados utilizando los proyectores $|m_z\rangle\langle m_z|$ definidos como:

$$|m_0\rangle\langle m_0| = \left\{M_0^0 = |0\rangle\langle 0|\,, M_0^1 = |1\rangle\langle 1|\right\}, \tag{6.2}$$

$$|m_1\rangle\langle m_1| = \left\{M_1^0 = |+\rangle\langle +|\,, M_1^1 = |-\rangle\langle -|\right\}, \tag{6.3}$$

donde $|\pm\rangle = \frac{1}{2}(|0\rangle \pm |1\rangle)$, y M_z^j permite adivinar que el bit en la posición z de $|x\rangle$ es un estado j, con $j = \{0, 1\}$.

Bajo estas condiciones, se estima la probabilidad media que M adivine correctamente el valor de uno de los bits de x, utilizando:

$$p_{AV} = p(b = j/x, z) = \langle x|\, M_z^j\, |x\rangle\,, \tag{6.4}$$

con esto, la probabilidad de recobrar correctamente cualquier bit de x estará dada por:

$$p_{AV} = cos(\pi/8)^2 = \frac{1}{2}(1 + 2cos(\pi/8)sen(\pi/8)) = 0{,}856. \tag{6.5}$$

El resultado anterior muestra como la probabilidad media de un sistema cuántico ($p_{AV} = 0{,}856$) [73], es mayor a la probabilidad media en un sistema clásico ($p_{AV}^c = 0{,}75$) [74]. Finalmente, la evaluación de estas probabilidades nos permitirán corroborar el estado cuántico de nuestro sistema, habilitando nuestra configuración para el sistema SDI a implementar.

6.1.2. Protocolo para generación de números aleatorios privados

Cada ronda del experimento produce un evento $(b|x, y, z)$ (emisión-detección), después de obtener N rondas se procede a:

1. El usuario estima la probabilidad de obtener b, dado el conjunto x, y, z, definida como $p(b|x, y > \lambda, z)$. Con la eliminación de las cuentas bloqueadas ($b = \emptyset$), el usuario puede obtener $p'(b|x, y > \lambda, z)$.

2. Se evalúa si hay aleatoriedad compartida entre los generadores x y z. Para esto, se estima la probabilidad media que M adivine correctamente el valor de uno de los bits de x, esto es: $p'_{AV} = \frac{1}{8}\sum_{x,z} p'(b = x_z/x, y > \lambda, z)$, donde x_z es el primer o segundo bit a adivinar de x. Además, con estos valores la eficiencia de detección (η), puede estimarse utilizando $\eta = \frac{\sum_{x,z}\sum_{b\in\{0,1\}} p(b|x,y>\lambda,z)}{\sum_{x,z}\sum_{b\in\{0,1,\emptyset\}} p(b|x,y>\lambda,z)}$. Con esta estadística, el usuario compara p'_{AV} con un umbral que depende de λ y η, evaluando la privacidad de la generación.

3. Con la privacidad comprobada en (2), el usuario obtiene una cadena de números aleatorios evaluando las salidas de $p(0/x, z)$.

6.1.3. Umbral para evaluación de privacidad

Si Eva es un agente externo quien fabrica y altera QRNG, entonces éste podría aprender a generar información compartida entre las entradas x y z. Para esto tiene dos opciones; (i) alimentado ambos QRNG con la misma semilla y/o (ii) haciendo que la elección en x envíe información a z generando una data conocida por dicho ente. El usuario fácilmente puede chequear (i), sin embargo (ii) puede generar una data aceptable por las pruebas estándares de aleatoriedad [70].

Por esto, la etapa B bloquea la ronda de medición desincronizando la data conocida por Eva, obligándole a re-sincronizar la data a generar. Para sincronizar, Eva envía un qubit con la información de la ronda en la que se encuentra. Si la probabilidad de bloqueo es R y el adversario requiere una confianza c que el qubit se recibe en M, entonces necesita $n1 = log_R(1 - c)$ rondas para volver a sincronizar .

Cuando Eva sincroniza, puede utilizar la aleatoriedad compartida hasta que B bloquee nuevamente. El número medio de rondas en este tiempo está dada por $n2 = \frac{1-R}{R}$.

En el periodo de sincronización $p'_{AV} = \frac{1}{2}$, debido a que no hay correlación entre b de M y x de P. Por tanto, con p'_{AV} el usuario podría evaluar si existe data compartida o no.

Sin embargo, Eva puede engañar al usuario generando un falso $p'_{AV} = 1$ para compensar la reducción en el sincronismo. Más aún, si Eva controla el detector, ésta puede ocultar el sincronismo con la ineficiencia del detector, y habilitarlo sólo en las rondas cuando la data esté sincronizada. Entonces, si la eficiencia de detección total es η, la probabilidad de habilitar el detector en una ronda con $p'_{AV} = \frac{1}{2}$ es:

$$\gamma = max \left\{ 0, \frac{\eta(n_1 + n_2) - n_2}{n_1} \right\}. \tag{6.6}$$

En base a la ecuación 6.6, la probabilidad de recuperar con éxito uno de los bit codificados queda como:

$$p_{AV}^{umbral} = \frac{\frac{1}{2}\gamma n_1 + n_2}{\gamma n_1 + n_2}, \tag{6.7}$$

donde p_{AV}^{umbral} está en función de c, R y la eficiencia observada η. Luego, si p'_{AV} es menor que (6.7), entonces el usuario puede concluir que no hay aleatoriedad compartida.

Por otro lado, considerando la figura 6.1, dependiendo de cada x Alice prepara un $|x\rangle$ en P. En M para un z dado se tiene:

1. Con frecuencia p_z, se proyecta la entrada con $|m_z = 0\rangle$ o $|m_z = 1\rangle$, obteniendo salidas $b = 0$ o $b = 1$ respectivamente.

2. Con frecuencia q_z^0, no se realiza medición sobre el qubit con la salida $b = 0$.

3. Con frecuencia q_z^1, no se realiza medición sobre el qubit pero la salida ahora es $b = 1$.

Considerando la condición normalizada de las probabilidades ($p_z + q_z^1 + q_z^0 = 1$), la aleatoriedad en los eventos $(b|x, z)$, medidos por la mínima entropía estará dada por:

$$H_\infty(b|x, z) = -p_z log_2(|\langle m_z = b|x\rangle|^2), \tag{6.8}$$

donde $|\langle m_z = b|x\rangle|^2$ es la probabilidad de proyectar $|m_z = b\rangle$ cuando el estado preparado es $|x\rangle$.

Como P y M son cajas negras, el usuario no conoce p_z, $|x\rangle$ ni $|m_z = b\rangle$, teniendo acceso sólo a la probabilidad $p(b|x,z)$, donde:

$$p(b|x,z) = q_z^b + p_z \left|\langle m_z = b|x\rangle\right|^2 . \tag{6.9}$$

El indicador de aleatoriedad usado en el protocolo es una lista $\vec{P}$ de 8 probabilidades $p(0/x,z)$. Después que el experimento esté completo, el usuario tiene cada $p(0|x,z)$ con confianza:

$$p(0|x,z)^{min} \leq p(0|x,z) \leq p(0|x,z)^{max}. \tag{6.10}$$

Entonces para obtener generación aleatoria, se realiza una minimización de (6.8) de 8 eventos $(0|x,z)$ bajo las restricciones en (6.10).

Se remarca que en nuestro protocolo, $\vec{P}$ permite al usuario certificar más aleatoriedad que cualquier indicador usado en trabajos previos, tales como: la probabilidad media de éxito $p_{AV} = \frac{1}{8}\sum_{x,z} p(0|x,z)$ [36, 75], o la probabilidad de peor caso $p_{wc} = min_{x,z} p(0|x,z)$ [76, 74].

6.2. Implementación experimental

El diagrama esquemático utilizado se muestra en la figura 6.2. Para generar las entradas aleatorias (x,y,z) utilizamos QRNGs comerciales [10], donde cada uno genera una cadena aleatoria constante. Se remarca la idea de que estos QRNG pueden dejar patrones de correlación no detectados por pruebas estándar [70].

Como se gráfica, de tres FPGAs el de la etapa de preparación es el maestro. Éste genera una señal de sincronismo para los dos esclavos restantes. En la etapa P se excita un modulador acusto-óptico (AOM), el cual dejará pasar un pulso de luz atenuada desde un láser continuo. Los pulsos ópticos son modulados utilizando de instrumentos ópticos pasivos, y cuatro moduladores espaciales de luz (SLMs) activos.

Para codificar los estados del qubit, utilizamos el *momento transversal lineal* de fotones individuales. Esto se logra proyectando máscaras sobre los SLMs, las que generan dos posibles caminos para el fotón transmitido [77].

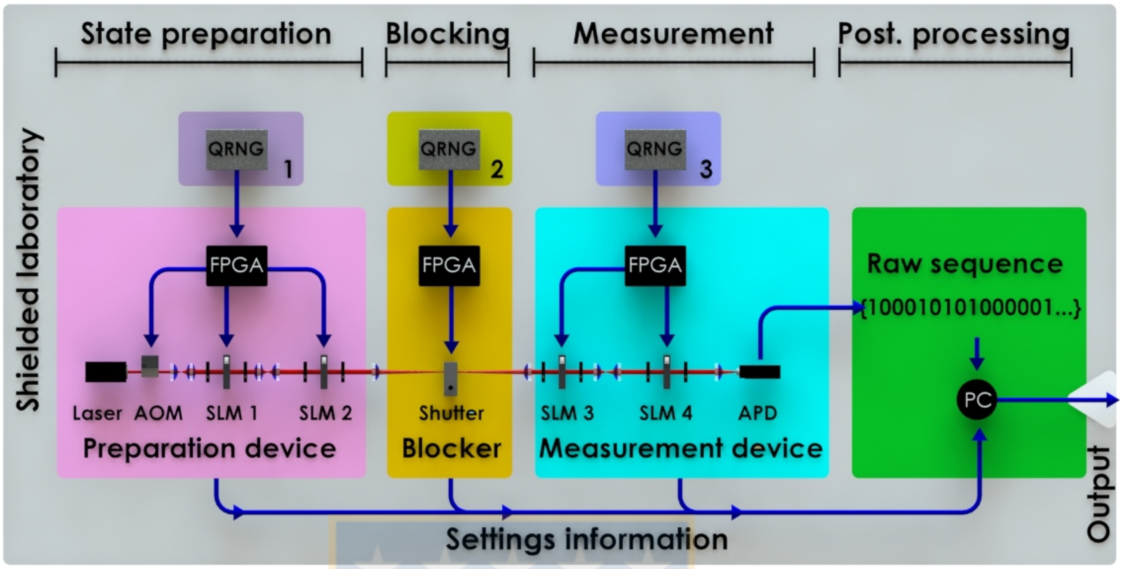


Figura 6.2: Configuración experimental para obtención de números aleatorios privados.

La generación de estados en P y las proyecciones de éstos en M, son implementados usando cuatro SLM_i (con $i \in \{1, 2, 3, 4\}$), funcionando con modulación en amplitud, y modulación en fase [9]. Cada interacción contempla una emisión de un pulso atenuado a 30Hz de repetición.

La modulación aplicada a cada SLM es excitada por la señal de sincronismo maestro junto a un retraso en cada FPGA. Asegurando el sincronismo global entre la emisión del pulso, la modulación (estado-proyección) y la generación de una ventana de detección.

Por otro lado, las máscaras de generación de estados, bloqueo y proyecciones son seleccionadas por las cadenas de números aleatorios comerciales. Como se menciona, la etapa B tiene un umbral (λ) integrado al algoritmo dentro de la FPGA de dicha etapa.

6.3. Resultados obtenidos

En nuestro experimento, para garantizar que no exista aleatoriedad compartida, utilizamos una eficiencia de detección de $\eta = 0{,}06$ y una tasa de bloqueo con $R = 0{,}99$.

Los umbrales de privacidad en función de la tasa de bloqueo y η se muestran en la figura 6.3. Claramente, se aprecia como nuestra cadena aleatoria está sobre el umbral correspondiente a la eficiencia de $\eta = 0{,}06$, certificando aleatoriedad privada. Por otro lado, la figura 6.3 muestra como para $\eta > 0$, siempre hay una $R < 1$ tal que se observe un $p'_{av} > 0{,}5$, lo que garantiza con un $99\,\%$ de confianza que no hay aleatoriedad compartida.

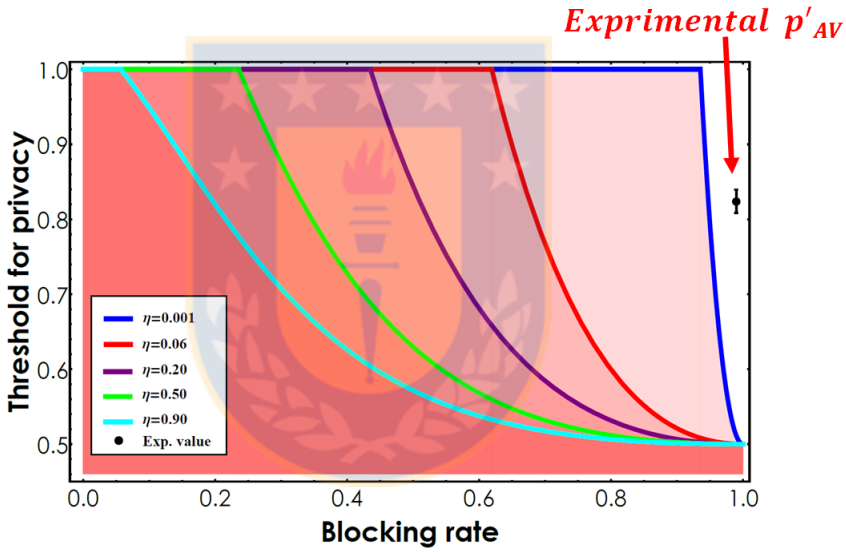


Figura 6.3: Resultados experimentales evaluados sobre p_{AV}^{umbral}. El umbral p_{AV}^{umbral} es obtenido para distintas eficiencia de detección (η) en función de la tasa de bloqueo R, el factor de confianza utilizando fue $c = 0{,}99$. Utilizando una tasa de bloqueo $R = 99\,\%$ se descarta aleatoriedad compartida, incluso para muy baja eficiencia de detección ($\eta = 0{,}001$)

Además, el resultado p'_{av} obtenido por sobre el umbral para $\eta = 0{,}001$, indica que nuestra configuración no depende de la eficiencia de detección para obtener aleatoriedad privada, haciendo de este diseño un generador de números aleatorios independientes de la eficiencia de detección.

Finalmente, la figura 6.4 muestra la calidad óptica de nuestro experimento, donde la probabilidad experimental $p'(0/x, y > \lambda, z)$ se muestra acorde con las predicciones de la mecánica cuántica (ver ecuación 6.5). Con esto, en cada ronda $0{,}0093$ bits aleatorios son certificados como privados, y con una tasa de $0{,}28Hz$, se obtuvo una secuencia aleatoria χ de 10^5bits de largo.

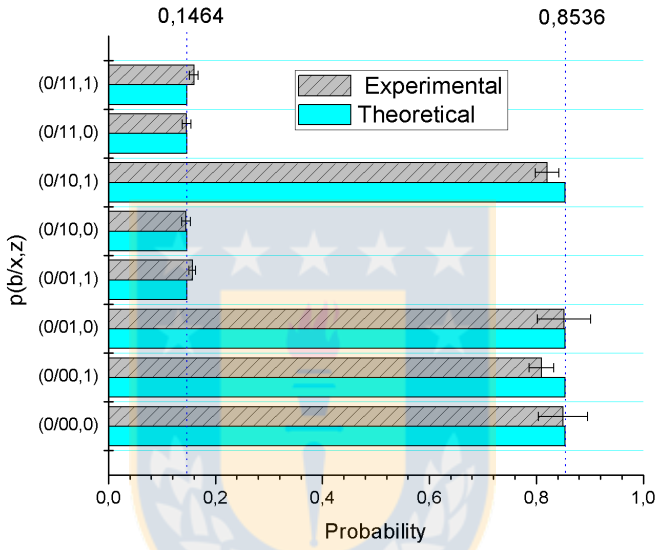


Figura 6.4: Probabilidades teóricas y experimentales obtenidas para una configuración QRAC $2 \rightarrow 1$.

En conclusión, hemos demostrado experimentalmente un protocolo para generar números aleatorios privados, el que puede ser más seguro que los convencionales QRNG y a la vez práctico para aplicaciones de un usuario común, por el hecho de no depender de alta eficiencia de detección [78].

CAPÍTULO 7

SISTEMA CUÁNTICO DE ALTA DIMENSIÓN PARA QKD

Capítulo 7

Sistema cuántico de alta dimensión para QKD

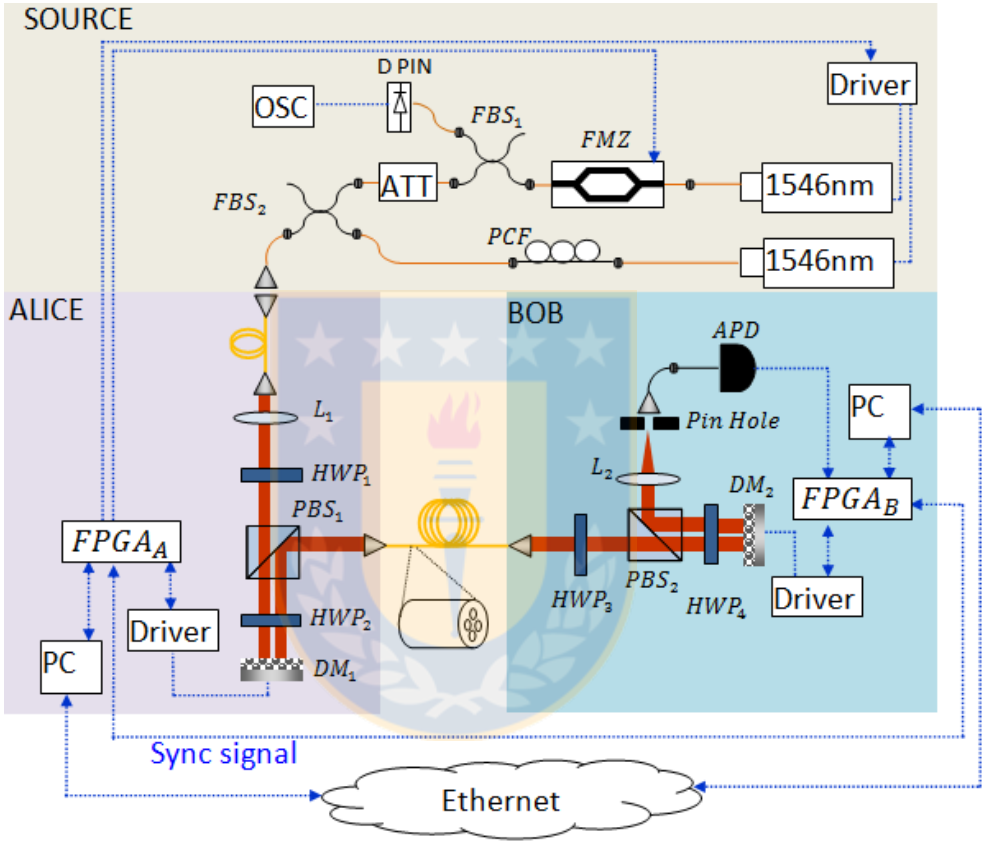
En comunicaciones digitales clásicas, los sistemas de alta dimensión maximizan la eficiencia del canal de comunicación. Sin embargo, la utilización de estados de alta-dimensión en información cuántica, tienen la ventaja que hay siempre un set de pruebas con resultado $(+1, -1)$, para la cual no importa como el sistema esté preparado, las predicciones de la teoría cuántica no pueden se reproducida con alguna teoría de variables ocultas no contextuales [79]. Además la utilización de estos sistemas son seguros ante ataques de terceros, incluso tolerado un QBER mayor al de un sistema de menor dimensión [44]. Estos sistemas han sido generados utilizando; energía tiempo [49], momento angular orbital [50] y momento transversal [9], entre otros.

Con la fibra óptica, la capacidad del canal de comunicación ha tenido un gran progreso las últimas décadas, utilizando técnicas como multiplexación; temporal, en longitud de onda, polarización y fase. En este contexto, el incremento de la capacidad utilizando multiplexación por división espacial (SDM), cobra interés con la utilización de la fibra multicore [37], lo que implica que éstas reemplazarán las fibras actuales en un futuro no muy lejano. Con esta idea implementaremos la primera generación de estados cuánticos de alta dimensión utilizando SDM sobre fibra multicore.

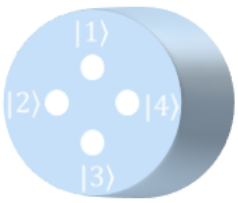
7.1. Sistema cuántico de alta dimensión utilizando fibra óptica multicore

El sistema completo se muestra en la figura 7.1.a, el cual está compuesto por una fuente, Alice, Bob y el canal cuántico que es simulado con una bobina de $250m$ de fibra multicore. La fuente es armada sobre fibra óptica monomodo y une dos láser de 1550nm, el primero para generar pulsos atenuados y el segundo para sensar la fase producida en Alice y Bob. Para generar los pulsos se utiliza un modulador MZ en fibra (FMZ), éste es conectado a un divisor de haz (FBS_1), una de sus salidas se conecta a un detector para monitorear la forma del pulso óptico a través de un osciloscopio (OSC), y la otra a un atenuador en fibra (ATT),

para finalmente ser conectado al FBS_2 de salida. La otra entrada del FBS_2 es conectada a un segundo láser, cuya polarización se controlará utilizando un control de polarización manual en fibra (PCF). La salida de la fuente es acoplada a un trozo de fibra multicore, produciendo los estados graficados en la figura 7.1.b.



(a)



(b)

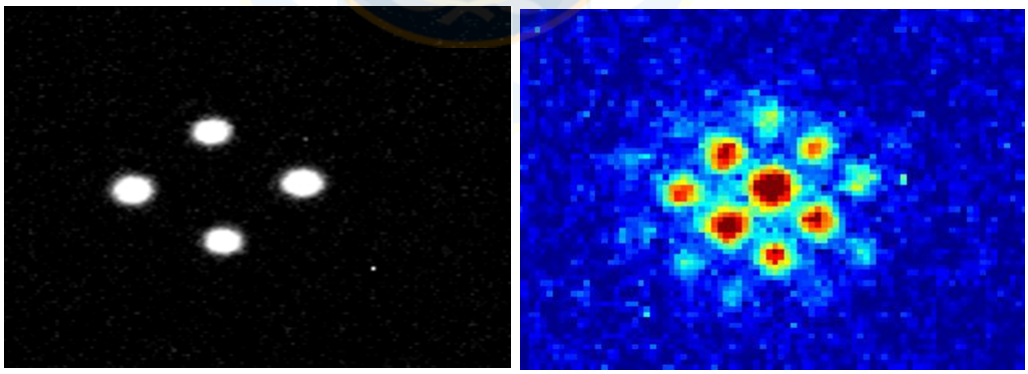
Figura 7.1: Generación de sistema cuántico con dimensión 4. a)Configuración experimental. b)Estados producido en en fibra óptica de cuatro núcleos.

En Alice, la luz del trozo de fibra multicore es desacoplada y colimada para tener emisión en espacio libre (utilizando la lente L_1), para luego pasar por una placa de media onda (HWP_1) (ver figura 7.1.a). En esta etapa se alinea el haz en polarización H (transmisión máxima por el PBS_1), luego el haz es rotado en $45°$ utilizando HWP_2 e incide sobre un espejo deformable (DM_1).

La reflexión del DM inserta una fase a cada núcleo, luego es rotada $45°$ (por HWP_2) obteniendo polarización vertical para reflejar máxima potencia por el PBS_1, siendo dirigida al acoplador del canal cuántico (250m fibra multicore).

En la recepción (Bob), después de desacoplar la luz de la fibra realiza la misma operación óptica que Alice, transmitiendo el resultado sobre una lente de salida (L_2). En el foco del sistema (contemplando la lente L_2), se inserta un filtro espacial (pin hole), el cual permite evaluar la interferencia entre los haces producidos.

El haz de salida es acoplado y conectado a un APD de fibra, para finalmente evaluar el sistema generado. En el plano focal se mide la interferencia producto de las fases producidas en Alice y Bob, mientras que en plano imagen se aprecia el patrón en intensidad de ésta. Estas imágenes se muestran en la figura 7.2, y fueron tomadas con una cámara infrarroja.



(a) (b)

Figura 7.2: Mediciones ópticas sobre la salida en Bob. a)Plano imagen, no se aprecia efecto crosstalk. b)Patrón de interferencia en el plano focal.

El espejo DM es controlado por un FPGA a través de un driver, el cual tiene una latencia variable menor a $0{,}5ms$. Para compensar la latencia, los FPGAs en Alice y Bob se sincronizan en base a la respuesta del driver, utilizando un canal bidireccional (ver figra 7.1.a), asegurando la modulación en ambos espejos antes de la emisión de pulsos atenuados, por este motivo la tasa de transición de estados se establece en $1000pulsos/s$.

Con la señal de sincronismo activada, el sistema puede emitir los pulsos en Alice (excitando el FMZ) y abrir una ventana de detección sobre el APD en Bob, evaluando con la modulación de fase estable en ambos espejos.

Finalmente, los datos de generación y detección son almacenados en los FPGAs y enviados a sus respectivos computadores (PC), los cuales a través de una conexión ethernet podrán ejecutar un algoritmo QKD.

Con esta configuración en fase es posible generar estados ortogonales para una base, y a su vez bases mutuamente imparciales. Por la dimensión es posible generar cinco MUBs, sin embargo basta con dos para producir QKD.

La figura 7.3, muestra como varía el patrón de interferencia entre el producto $(\theta_0^A \rightarrow \theta_0^B)$ y el producto $(\theta_0^A \rightarrow \theta_1^B)$, donde los primeros son paralelos y los segundos son ortogonales.

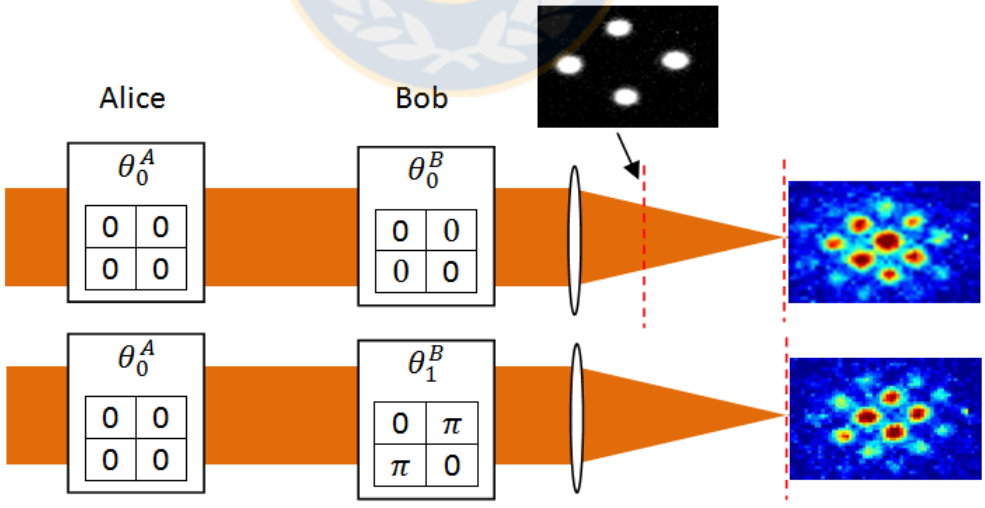


Figura 7.3: Modulación de fase en dimensión 4, para Alice y Bob.

7.1.1. Generación de ququart

Nuestro sistema modula la fase en cada núcleo de la fibra multicore, entonces al atenuar el haz generaremos sistemas cuánticos de dimensión 4 (ququart). Para esto, Alice a través de su FPGA apaga el láser de control y enciende el láser conectado al atenuador en fibra, preparando el sistema:

$$|\psi\rangle = c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle + c_4 |4\rangle = \sum_{k=1}^{4} c_j |k\rangle = \frac{1}{\sqrt{4}} \sum_{k=1}^{4} |k\rangle. \tag{7.1}$$

La modulación en el DM es de la forma:

$$|\phi\rangle = \frac{1}{2} \sum_{k=1}^{4} \mathrm{e}^{j\theta_k^A} |k\rangle \langle k|, \tag{7.2}$$

donde $\mathrm{e}^{j\theta_k^A}$ será la fase modulada por el DM en Alice.

Al interactuar (7.1) con (7.2), se produce:

$$|\varphi\rangle = \frac{1}{2} \sum_{k=1}^{4} \mathrm{e}^{j\theta_k^A} |k\rangle. \tag{7.3}$$

Por otro lado, Bob realiza la misma operación con (7.3), obteniendo:

$$|\varphi\rangle = \frac{1}{2} \sum_{k=1}^{4} \mathrm{e}^{j\left(\theta_k^A + \theta_k^B\right)} |k\rangle. \tag{7.4}$$

7.1.2. Resultados preliminares transmisión de ququart

Con el propósito de evaluar la calidad de los estado generados, utilizamos el índice fidelidad descrito como:

$$F = \frac{C_{E_n}}{\sum_{k=1}^{4} C_{E_k}}, \tag{7.5}$$

donde C_{E_n} son las cuentas en el punto focal, cuando Alice y Bob comparten la base y Bob proyecta el estado E_n.

Con esto se obtienen las gráficas de la figura 7.4, donde se aprecia una fidelidad promedio en las dos bases de $94\,\%$.

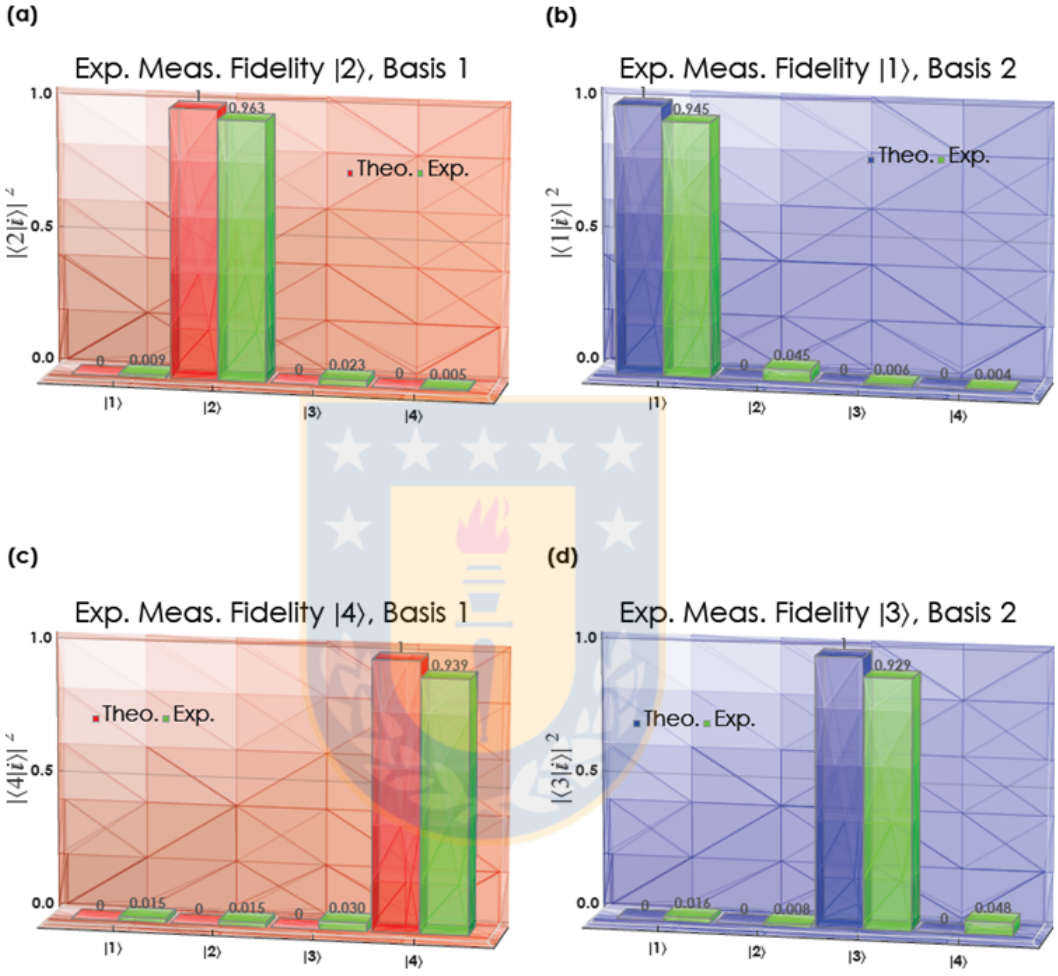


Figura 7.4: Evaluación de la fidelidad de los estados cuánticos generados por el sistema. Se evalúa la fidelidad para los estados generados, los cuales son proyectados sobre estados de la misma MUB, obteniendo una fidelidad promedio de $94\,\%$. a) Evaluación del estado E_2 base 1, donde $p(E_2^A) \approx \left|\langle E_2^A|E_i^B\rangle^2\right|$ con $i = \{1,2,3,4\}$. b) Evaluación del estado E_1 base 2. c) Evaluación del estado E_4 base 1. d)Evaluación del estado E_3 base 2.

Por otro lado, el QBER se define como:

$$QBER_{E_n} = \frac{\sum_{k=1}^{4} C_{E_{k\neq n}}}{\sum_{k=1}^{4} C_{E_k}}, \tag{7.6}$$

donde E_k son los estados de la misma base que E_n.

Como tenemos dos bases, llamaremos $qber_1$ y $qber_2$ a la media de las QBER por MUB, para finalmente obtener un $qber_T$ equivalente a la media entre estos. Al realizar sesión en función del tiempo, se obtienen los resultados mostrados en la figura 7.5, en ésta imagen se aprecia como el error varía en función del tiempo, esto es producto de las fluctuaciones térmicas, eléctricas y producto de vibraciones del ambiente, sobre el sistema y la fibra multicore de $250m$.

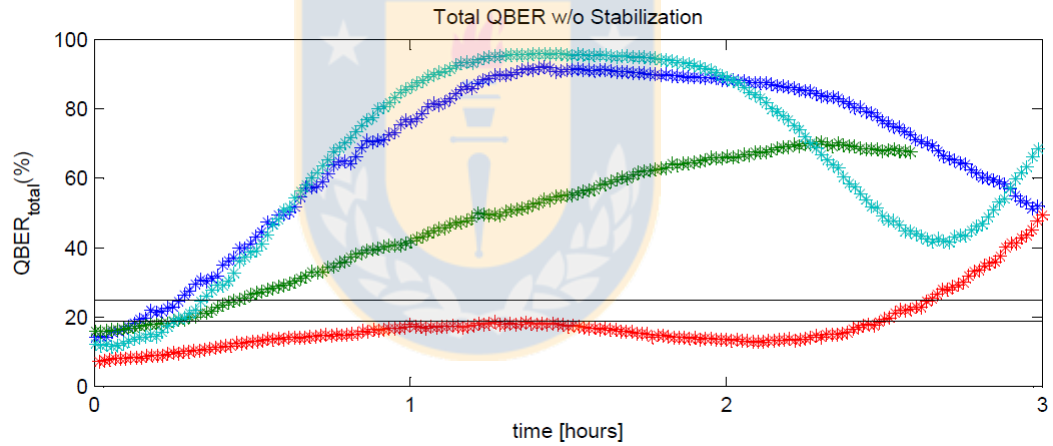


Figura 7.5: QBER experimental en configuración pasiva.

Para compensar el error en fase, sobre el DM de Bob utilizamos un control denominado *maximum-power-point-tracking* específicamente la técnica perturbar y observar, para esto en Alice se enciende el láser no atenuado. Cuando el láser de control está encendido, primero se fija el estado E_0 en Alice y Bob respectivamente, luego se varía por pasos discretos el valor en fase en un espejo del DM_2, de forma cíclica completando la variación para los 4 espejos. Según las cuentas obtenidas, el algoritmo se detiene cuando la configuración compensada que presente la mayor cantidad de cuentas ($p(E_0^A) \approx \left|\langle E_0^A | E_0^B \rangle^2\right| = 1$). Esto asegura que el estado E_0^A está en fase con E_0^B, lo que implica que los valores de las MUBs podrán generar su desfase propio, volviendo a obtener la fidelidad inicial.

Cabe señalar que algoritmo se ejecuta utilizando el láser de control, por lo que este se apaga al finalizar la compensación de fase.

El error obtenido con fase compensada en función del tiempo se muestra en la figura 7.6, en ésta se aprecia como el QBER es inferior al $18{,}93\,\%$, que es el límite para generar clave segura [44]. El resultado anterior permite concluir que el sistema está habilitado para generar claves utilizando QKD [80].

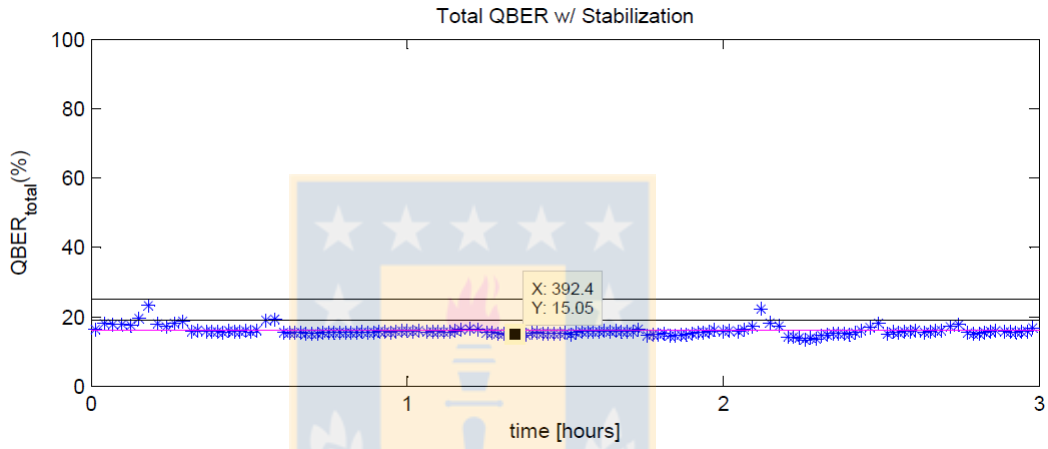


Figura 7.6: QBER experimental en configuración utilizando control activo.

CAPÍTULO 8

CONCLUSIONES

Capítulo 8

Conclusiones

8.1. Conclusión General

Las configuraciones experimentales para comunicación cuántica deben diseñarse para ser utilizadas en largas distancias y adecuándose a los enlaces de comunicación existentes. Por otro lado, actualmente es factible emitir y detectar estados cuánticos utilizando fotones. Sin embargo, las pérdidas de potencia, ruido y perturbaciones sobre las propiedades del fotón dentro de un enlace de fibra óptica generan desafíos experimentales para enlaces cuánticos. En este trabajo de tesis, a través del diseño avanzado en dispositivos de lógica programable (FPGA), logramos generar enlaces cuánticos de larga distancia en base a fibra óptica comercial y habilitar sistemas de procesamiento de información cuántica.

8.2. Conclusiones Específicas

Configuraciones estándar para entrelazamiento cuántico energía-tiempo, contemplan inseguridad intrínseca producto de un loophole geométrico. En este trabajo mostramos por primera vez que el entrelazamiento cuántico energía-tiempo, puede ser distribuido sobre una configuración alterna denominada hug, cuya geometría cierra el loophole mencionado, sobre enlaces de largas distancias utilizando fibra óptica comercial. Además, en base a una violación de la desigualdad de Bell por sobre 2.94 desviaciones estándar, certificamos un enlace cuántico bajo la configuración mencionada, utilizado interferómetros de 3.7km de fibra óptica instalada sobre la Universidad de Concepción.

Estos resultados se obtuvieron unicamente tras el aumento de la visibilidad de estados cuánticos y el control activo de fase sobre el enlace de fibra óptica. El aumento de visibilidad mencionado, se obtiene producto de la filtración de cuentas accidentales y disminución del error electrónico en el dispositivo contador de coincidencias basado en FPGA. Además, las ventajas de nuestro diseño fueron corroborados al aumentar la fidelidad de la violación

a CHSH de tres etapas. Nuestros resultados se consolidan como una demostración práctica que el entrelazamiento energía-tiempo, es verdaderamente factible para realización de comunicación segura, sobre infraestructura de telecomunicaciones existentes.

Por otro lado, en base al protocolo de generación de aleatoriedad cuántica propuesto por Pawlowski, nuestros resultados muestran que la configuración implementada no depende de la eficiencia de detección para obtener aleatoriedad privada, haciendo de este diseño un generador de números aleatorios independientes de la eficiencia de detección. Con esto, hemos demostrado experimentalmente un protocolo para generar números aleatorios privados, el que puede ser más seguro que los convencionales QRNG y a la vez práctico para aplicaciones de un usuario común, por el hecho de no depender de alta eficiencia de detección.

Finalmente, se implementa un sistema cuántico de dimensión 4 sobre fibra óptica multicore, donde a través de un control *maximum-power-point-tracking* sobre la fase relativa entre los núcleos de la fibra, se obtiene un QBER inferior al $19\,\%$, que es el límite para generar clave segura, demostrando la factibilidad de implementar un protocolo de QKD sobre nuestro diseño.

BIBLIOGRAFÍA

Bibliografía

[1] Simon Singh, The Code Book: HOW TO MAKE IT, BREAK IT, HACK IT, CRACK IT, Delacorte Press, (2002).

[2] Ladd, T. D., F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, Quantum computers, Nature (London), 464, 45, (2010).

[3] Hadfield, Robert H, Single photon detectors for optical quantum information applications, Nat Photon, 3, 1749, (2009).

[4] M. D. Eisaman, J. Fan, A. Migdall, S. V. Polyakov, Invited Review Article: Single photon sources and detectors, Rev. Sci. Instrum. 82, 071101, (2011).

[5] Wootters, W. K. and Zurek, W. H., A single quantum cannot be cloned, Nature, 299, 802 , (1982).

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

[7] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, India, (IEEE, New York, 1984), 175, (1984).

[8] C. H. Bennett,Quantum cryptography using any two states, Phys. Rev. Lett., 68, 3121, (1992).

[9] Etcheverry S, Cañas G, Gómez E S, Nogueira W A T, Saavedra C, Xavier G B and Lima G, Quantum key distribution session with 16 dimensional photonic states, Sci. Rep., 3, 2316, (2013).

[10] Rarity, J. G. , Owens, P. C. M. and Tapster, P. R. Quantum random number generation and key sharing., J. Mod. Opt., 41, 2435, (1994).

[11] Artur K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett, 67, 661 , (1991).

[12] J. S. Bell, On the Einstein Podolsky Rosen Paradox, Physics, 1, 195, (1964).

[13] J. F. Clauser, M. A. Horne, A. Shimonyand, R. A. Holt, Proposed experiment to test local hidden variable theories, 23, 880, (1969).

[14] S. L. Braunstein and C. M. Caves. Wringing out better Bell inequalities. Ann. Phys. (NY) 202, 22, (1990).

[15] J. A. Larsson, Loopholes in Bell inequality tests of local realism, J. Phys. A: Math. Theor., 47, 424003, (2014).

[16] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature, 526, 682, (2015).

[17] Adán Cabello, Alessandro Rossi, Giuseppe Vallone, Francesco De Martini, and Paolo Mataloni, Proposed Bell Experiment with Genuine Energy Time Entanglement, Phys. Rev. Lett., 102, 040401, (2009).

[18] J. D. Franson, Bell inequality for position and time, Phys. Rev. Lett. 62, 2205 , (1989).

[19] Sven Aerts, Paul Kwiat, Jan-Ake Larsson, and Marek Zukowski, Two Photon Franson Type Experiments and Local Realism, Phys. Rev. Lett., 83, 2872 (1999).

[20] G. Lima,1 G. Vallone, A. Chiuri, A. Cabello, and P. Mataloni. Experimental Bell inequality violation without the postselection Loopholes,Phys. Rev. A., 81, 040101, (2010).

[21] G. B. Xavier and J. P. von der Weid, Stable single photon interference in a 1 km fiber optic Mach Zehnder interferometer with continuous phase adjustment, Opt. Lett., 36, 1764, (2011).

[22] M.B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, F. J. Mendieta, Integrating a QPSK Quantum Key Distribution Link, ECOC2006 Conference Proceeding, France, (2006).

[23] Hong Fei Zhang, Jian Wang, Ke Cui, Chun Li Luo, Sheng Zhao Lin, Lei Zhou, Hao Liang, Teng Yun Chen, Kai Chen, and Jian Wei Pan, A Real Time QKD System Based on FPGA, Journal Lightwave Technol., 30, 3226, (2012).

[24] K. Cui, H. F. Zhang, A real time design based on FPGA for Expeditious Error Reconciliation in QKD system , IEEE Transactions on Information Forensics and Security, 8, 184, (2013).

[25] S. Gaertner, H. Weinfurter, and C. Kurtsiefer, Fast and compact multichannel photon coincidence unit for quantum information processing, Rev. Sci. Instrum., 76, 123108, (2005).

[26] Giancarlo Sportelli, et al. ,Low resource synchronous coincidence processor for positron emission tomography, Nuclear Instruments and Methods in Physics Research A, pp 199 201,(2011)

[27] D. Branning, S. Khanal, Y. H. Shin, B. Clary and M. Beck, Note: Scalable multiphoton coincidence counting electronics, Rev. Sci. Instrum. 82, 016102 (2011).

[28] Raphael C. Pooser, Dennis D. Earl, Philip G. Evans, Brian Williams, Jason Schaake and Travis S. Humble, FPGA based gating and logic for multichannel single photon counting, J. Mod. Opt., 59, 1500, (2012).

[29] Park, B. K., Kim, Y., Kwon, O., Han, S., Moon, S., High-performance reconfigurable coincidence counting unit based on a field programmable gate array. Appl. Opt. 54, 4727 (2015).

[30] Parnell, K. , Mehta, N, Programmable Logic Design Quick Start Handbook. 4th ed. [s.l.]: Xilinx Inc., (2003).

[31] Spartan 6 FPGA SelectIO ResourcesUser Guide Spartan UG381, 6 , (2014).

[32] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, Quantum key distribution with 1.25 Gbps clock synchronization, Opt. Express, 12, 2011, (2004).

[33] Mink A, Bienfang J C, Carpenter R, Ma L, Hershman B, Restelli A and Tang X, Programmable instrumentation and gigahertz signaling for single-photon quantum communication systems New J. Phys., 11, 045016, (2009).

[34] Shen, Q., Liao, S., Wang, J., Liu, W., Peng, C., and An, Q. . An FPGA-Based TDC for Free Space Quantum Key Distribution, IEEE Transactions on Nuclear Science, 60, 3570, (2013).

[35] X. Lu, L. Zhang, Y. Wang, W. Chen, D. Huang, D. Li, S. Wang, D. He, Z. Yin, Y. Zhou, C. Hui, and Z. Han, FPGA based digital phase-coding quantum key distribution system, Sci. China: Phys., Mech. Astron. 58, 120301, (2015).

[36] Pawlowski, M., Brunner, N.: Semi device independent security of one way quantum key distribution. Phys. Rev. A, 84, 010302, (2011).

[37] D. J. Richardson, J. M. Fini and L. E. Nelson, Space-division multiplexing in optical fibres, Nat Photon, 7, 354, (2013).

[38] C. E. Shannon, Communication Theory of Secrecy Systems, Bell Syst. Tech. J., 28, 656, (1949).

[39] Mitali VK, Sharma A, A survey on various cryptography techniques. IJETTCS, 3, 2278, (2014).

[40] Peter W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing, 26, 1484, (1997).

[41] Vernam, G., Cipher printing telegraph systems for secret wire and radio telegraphic communications, J. Am. Institute of Electrical Engineers, 45, 109, (1926).

[42] M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 10, (2010).

[43] W. K. Wootters and B. D. Fields, Optimal state-determination by mutually unbiased measurements, Ann. Phys. New York, 191, 363, (1989).

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

[45] Bennett, Ch.H., G. Brassard, C. Crepeau, and U.M. Maurer, IEEE Trans. Information , 41, 1915, (1995).

[46] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A, 123, 257, (1987).

[47] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A, 126, 303, (1988).

[48] A. Peres, How to differentiate between non-orthogonal states Phys. Lett. A, 128, 19, (1988).

[49] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Quantum Cryptography Using Entangled Photons in Energy-Time Bell States, Phys. Rev. Lett., 84, 4737, (2000).

[50] M. Mirhosseini1, O. S. Magana-Loaiza, M. N. O Sullivan, B. Rodenburg, M. Malik, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New J. Phys., 17, 033033, (2015).

[51] Eric Yao, Sonja Franke-Arnold, Johannes Courtial, Miles J. Padgett, and Stephen M. Barnett, Observation of quantum entanglement using spatial light modulators, Opt. Express, 14, 13089, (2006).

[52] Horodecki, R., Horodecki, P., Horodecki, M. and Horodecki, K. Quantum entanglement. Rev. Mod. Phys., 81, 865 (2009).

[53] A. Einstein, B. Podolsky, and N. Rosen, Can Quantum-Mechanical description of physical reality be considered complete?. Phys. Rev. 47, 777, (1935).

[54] I Supic, R Augusiak, A Salavrakos yA Acín, Self-testing protocols based on the chained Bell inequalities, New J. Phys. 18, 167, (2016).

[55] Alain Aspect, Jean Dalibard, and Gérard Roger, Experimental Test of Bell's Inequalities Using Time-Varying Analyzers. Phys. Rev. Lett., 49, 1804, (1982).

[56] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger, Violation of Bell's inequality under strict Einstein locality conditions, Phys. Rev. Lett. 81, 5039, (1998).

[57] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, Bell Inequality Violation with Two Remote Atomic Qubits. Phys. Rev. Lett. 100, 150404, (2008).

[58] M. D. Eisaman, J. Fan, A. Migdall, S. V. Polyakov, Invited Review Article: Single-photon sources and detectors, Rev. Sci. Instrum. 82, 071101, (2011).

[59] Ryan E. Warburton , et al, Quantum correlations in position, momentum, and intermediate bases for a full optical field of view, Phys. Rev. A, vol 85,p 013827,(2012)

[60] Leach, J., et al, Single-photon position to time multiplexing using a fiber array, Opt. Express, vol 19,pp2670-2675,(2011), 10.1364/OE.19.002670

[61] Kurtsiefer, et al, Generation of correlated photon pairs in type-II parametric down conversion-revisited, J. Mod. Opt., 48, 1997, (2001).

[62] Lei Zhao and Xueye Hu and Shubin Liu and Jinhong Wang and Qi Shen and Huanhuan Fan and Qi An, The Design of a 16-Channel 15 ps TDC Implemented in a 65 nm FPGA, Nuclear Science, IEEE Transactions on, vol 60, pp 3532-3536, (2013).

[63] L. Zehnder, Ein Neuer Interferenzrefraktor, Zeitschrift fur Instrumentenkunde. 11, 275, (1891).

[64] L. Mach., Über einer Interferenzrefractor, Zeitschrift fur Instrumentenkunde, 12, 89, (1982).

[65] W. S. Levine, The control handbook, CRC Press, 1, (2000).

[66] A. Cuevas, G. Carvacho, G. Saavedra, **J. Cariñe**, W.A.T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima and G.B. Xavier, Long-distance distribution of genuine energy-time entanglement, **Nat Commun**, 4, 11, **(2013)**.

[67] Clauser, J. F., and A. Shimony, Bell's theorem: experimental tests and implications, Rep. Prog. Phys. 41, 1881, (1978).

[68] G. Carvacho, **J. Cariñe**, G. Saavedra, A. Cuevas, J. Fuenzalida, F. Toledo, M. Figueroa, A. Cabello, J.A. Larsson, P. Mataloni, G. Lima, and G. B. Xavier, **Phys. Rev. Lett**, 115, 030503 **(2015)**.

[69] T. Kim, M. Fiorentino, and F. N. C. Wong, Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer, Phys. Rev. A, 73, 012316, (2006).

[70] National Institute of Standards and Technology (NIST), http://csrc.nist.gov/groups/ST/toolkit/rng/index.html, (2015).

[71] Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T. A. and Monroe, C. Random numbers certified by Bells theorem, Nature, 464, 1021, (2010).

[72] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. Quantum random access codes using single d-level systems. Phys. Rev. Lett., 114, 170502, (2015).

[73] Yao Y, Li H-W, Zou X-B, Huang J-Z, Zhang C-M, Yin Z-Q, Chen W, Guo G-C and Han Z-F 2012 Quantum discord in quantum random access codes and its connection to dimension witnesses Phys. Rev. A 86, 062310, (2012).

[74] Ambainis, A., Nayak, A., Ta-Shma, A. and Vazirani, U. Dense quantum coding and quantum finite automata. J. ACM 49, 496 (2002).

[75] Li, H.W., Yin, Z.-Q., Wu, Y.C., Zou, X.B., Wang, S., Chen, W., Guo, G.-C. and Han, Z. F. Semi-device-independent random-number expansion without entanglement. Phys. Rev. A 84, 034301 (2011).

[76] Dall Arno, M., Passaro, E., Gallego, R., Pawlowski, M. and Acín, A. Attacks on semi-device independent quantum protocols. Quant. Inf. Comp. 15, 0037 (2015).

[77] Lima, G., Vargas, A., Neves, L., Guzm´an, R. and Saavedra, C., Manipulating spatial qudit states with programmable optical devices. Opt. Express, 17, 10688, (2009).

[78] Gustavo Cañas, **Jaime Cariñe**, Esteban S. Gómez, Johanna F. Barra, Adán Cabello, Guilherme B. Xavier, Gustavo Lima, Marcin Pawlowski, Experimental quantum randomness generation invulnerable to the detection loophole, **arXiv:1410.3443v2**, **(2014)**.

[79] Asher Peres, Quantum Theory: Concepts and Methods (KLUWER ACADEMIC PUBLISHERS), (2002).

[80] Gustavo Cañas, N. Vera, **Jaime Cariñe**, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers, **arXiv:1610.01682v2**, **(2016)**.

APÉNDICE

Apéndice A

Producción

En el transcurso de este trabajo de tesis se han obtenido los siguientes resultados:

Artículo en preparación

- **J. Cariñe**, S. Gómez, Esteban. S. Gómez A. Wolf, L. Araneda, G. Lima, M. Figueroa, and G.B. Xavier, Simultaneous measurement of multi-width coincidence windows using a low cost and high performance FPGA-based coincidence counter. (2016).

Artículos enviados a revistas científicas

- Gustavo Cañas, N. Vera, **Jaime Cariñe**, P. González, J. Cardenas, P. W. R. Connolly, A. Przysiezna, E. S. Gómez, M. Figueroa, G. Vallone, P. Villoresi, T. Ferreira da Silva, G. B. Xavier, and G. Lima, High-dimensional decoy-state quantum key distribution over 0.3 km of multicore telecommunication optical fibers, **Nat Commun**, (2016).

- Gustavo Cañas, **Jaime Cariñe**, Esteban S. Gómez, Johanna F. Barra, Adán Cabello, Guilherme B. Xavier, Gustavo Lima, Marcin Pawlowski, Experimental private quantum randomness generation invulnerable to the detection loophole, **SREP-16-41808**, **(2016)**.

Artículos publicados en revistas científicas

- Gustavo Cañas, Evelyn Acuña, **Jaime Cariñe**, Johanna F. Barra, Esteban S. Gómez, Guilherme B. Xavier, Gustavo Lima, and Adán Cabello, Experimental demonstration of the connection between quantum contextuality and graph theory, **Phys. Rev. A**, 94, 012337, **(2016).**

- G. Carvacho, **J. Cariñe**, G. Saavedra, A. Cuevas, J. Fuenzalida, F. Toledo, M. Figueroa, A. Cabello, J.A. Larsson, P. Mataloni, G. Lima, and G. B. Xavier, **Phys. Rev. Lett**, 115, 030503 **(2015)**.

- A. Cuevas, G. Carvacho, G. Saavedra, **J. Cariñe**, W.A.T. Nogueira, M. Figueroa, A. Cabello, P. Mataloni, G. Lima and G.B. Xavier, Long-distance distribution of genuine energy-time entanglement, **Nat Commun**, 4, 11, **(2013)**.

Apéndice B

El qubit

En este Apéndice se muestra con mayor detalle la representación de un qubit sobre la esfera de Bloch. El qubit es un sistema cuántico perteneciente a un espacio de Hilbert ($\mathcal{H}$) con dimensión 2, el cual es un espacio vectorial finito que incluye el producto escalar. Un qubit puede ser representado por:

$$|\psi\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle , \tag{B.1}$$

donde α_0 y β_0 son complejos, por tanto los podemos reescribir como:

$$\alpha_0 = \alpha e^{i\phi_\alpha}, \text{ y } \beta_0 = \beta e^{i\phi_\beta}, \tag{B.2}$$

donde ϕ_α y ϕ_β son fases en dichos complejos. Al reemplazar (B.2) sobre (B.1) se obtiene:

$$\begin{aligned} |\psi\rangle &= \alpha e^{i\phi_\alpha} |0\rangle + \beta e^{i\phi_\beta} |1\rangle , \\ &= e^{i\phi_\alpha} \left(\alpha |0\rangle + \beta e^{i(\phi_\beta - \phi_\alpha)} |1\rangle\right) , \end{aligned} \tag{B.3}$$

donde ϕ_α representa una fase global del sistema, mientras que $\phi_\beta - \phi_\alpha$ representa una fase entre los estados $|0\rangle$ y $|1\rangle$, al cual denominaremos solamente ϕ. Reescribiendo la ecuación B.3 como: $|\psi\rangle = e^{i\phi_\alpha} |\psi_0\rangle$ y considerando la probabilidad $p = |\langle\psi|\psi\rangle|^2$, si el producto interno de $|\psi\rangle$ está dado por $\langle\psi|\psi\rangle = e^{i(\phi_\alpha - i\phi_\alpha)} \langle\psi_0|\psi_0\rangle = \langle\psi_0|\psi_0\rangle$, entonces la probabilidad queda $p = |\langle\psi_0|\psi_0\rangle|^2$, lo que implica que la fase global ϕ_α no tiene efectos observables, y por tanto puede ser ignorada.

Con esta reducción podemos dibujar los ejes en un sistema cartesiano como muestra la figura B.1.

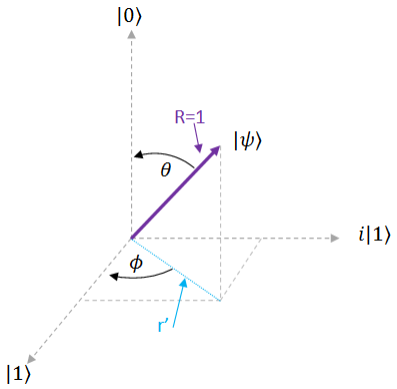


Figura B.1: El qubit y coordenadas polares.

Según la figura B.1, el qubit $|\psi\rangle$ puede representarse como:

$$|\psi\rangle = Rcos(\theta)\,|0\rangle + \left(r^{'}cos(\phi)\,|1\rangle + r^{'}sen(\phi)i\,|1\rangle\right). \tag{B.4}$$

Considerando que $R = 1$ y $r^{'} = Rsen(\theta)$, entonces la ecuación B.4, se reescribe como:

$$|\psi\rangle = cos(\theta)\,|0\rangle + sen(\theta)\,(cos(\phi) + isen(\phi))\,|1\rangle = cos(\theta)\,|0\rangle + sen(\theta)e^{i\phi}\,|1\rangle\,, \tag{B.5}$$

donde $cos(\theta)$ y $sen(\theta)$ representan los valores de las variables α y β de la ecuación B.3 respectivamente.

La esfera de Bloch se obtiene estableciendo los estados $|0\rangle$ y $|1\rangle$ como polos de dicha esfera tal como muestra la figura B.2, lo que implica que $0 \leq \theta \leq \pi$, luego la ecuación B.5 puede ser reescrita como:

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + sen(\theta/2)e^{i\phi}\,|1\rangle\,. \tag{B.6}$$

Utilizando la ecuación B.6, podemos obtener los estados mostrados en la tabla B.1. Como se aprecia en la tabla, esta esfera provee un amplio significado de la visualización de estados de un qubit individual, debido a que permite observar estados pertenecientes a las matrices de Pauli, los que se encuentran en cada polo de la esfera de Bloch.

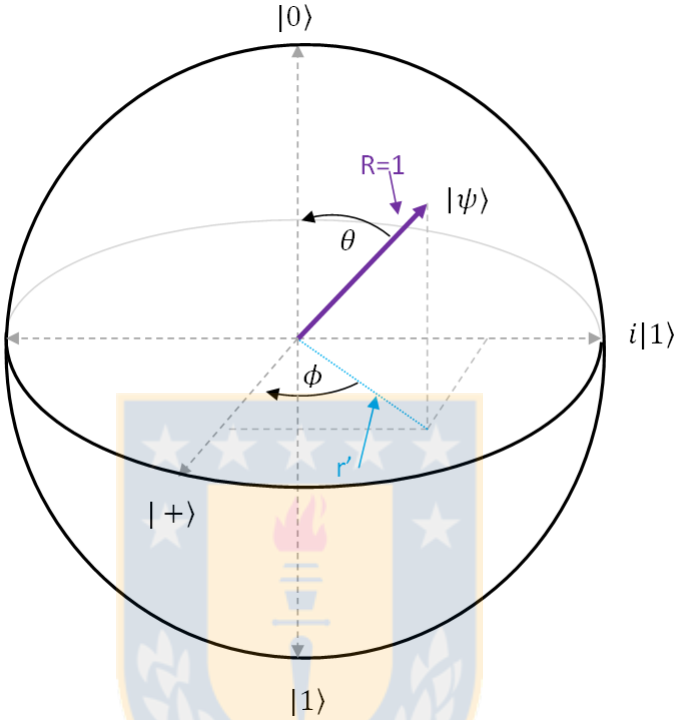


Figura B.2: El qubit y coordenadas polares.

θ	ϕ	$\|\psi\rangle$	Pauli matrices
0	0	$\|0\rangle$	σ_x
π	0	$\|1\rangle$	σ_x
$\frac{\pi}{4}$	$\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	σ_y
$\frac{\pi}{4}$	$-\frac{\pi}{2}$	$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	σ_y
$\frac{\pi}{4}$	0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	σ_z
$-\frac{\pi}{4}$	0	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	σ_z

Tabla B.1: Estados obtenidos dentro de la esfera de Bloch.

Apéndice C

Los postulados de la mecánica cuántica

Los postulados de la mecánica cuántica (MC) fueron obtenidos después de un largo proceso de prueba y error, éstos conectan el mundo físico con el formalismo matemático de la MC [42].

Primer postulado

Cualquier sistema físico aislado tiene un espacio vectorial complejo y con producto interno, conocido como espacio de estados del sistema. Este sistema es completamente descrito por dicho espacio vectorial, el cual es un vector unitario en el espacio de estados del sistema, esto es:

$$\forall \left|\psi\right\rangle \in \mathcal{H} : \exists \left\langle\psi|\psi\right\rangle / \left\langle\psi|\psi\right\rangle = 1, \tag{C.1}$$

donde $\langle\psi|$ es el sistema dual a $|\psi\rangle$, y $\langle\psi|\psi\rangle$ representa el producto interno entre un sistema y su dual. Por ejemplo, sea el sistema:

$$\left|\psi\right\rangle = \alpha \left|0\right\rangle + \beta \left|1\right\rangle . \tag{C.2}$$

Considerando $|\psi\rangle$ como un estado puro $\alpha^2 = \beta^2$, se tiene:

$$\begin{aligned} \left\langle\psi|\psi\right\rangle &= 1, \\ 1 &= (\alpha \left\langle 0\right| + \beta \left\langle 1\right|)(\alpha \left|0\right\rangle + \beta \left|1\right\rangle), \\ 1 &= \alpha^2 \left\langle 0|0\right\rangle + \alpha\beta \left\langle 0|1\right\rangle + \beta\alpha \left\langle 1|0\right\rangle + \beta^2 \left\langle 1|1\right\rangle , \\ 1 &= \alpha^2 + \beta^2, \end{aligned} \tag{C.3}$$

como $\alpha^2 = \beta^2$, entones $\alpha = \beta = \frac{1}{\sqrt{2}}$. Considerando el resultado anterior, la ecuación (C.2) se reescribe como:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right). \tag{C.4}$$

Segundo postulado

La evolución de un sistema cuántico que no interactua con otro de ninguna forma, está descrita por una transformación unitaria.

$$|\psi'\rangle = U |\psi\rangle . \tag{C.5}$$

Esto es, el estado $|\psi\rangle$ en t_1 es relativo al estado $|\psi'\rangle$ en un tiempo t_2 por un operador unitario U, el cual depende sólo de los tiempos t_1 y t_2.

Tercer postulado

Las medidas cuánticas son descritas por un grupo M_m de **operadores de medición** lineales y hermíticos, donde m hace referencia al resultado que podría ocurrir en el experimento.

Si el estado del sistema cuántico es $|\psi\rangle$ inmediatamente antes de la medición, entonces la probabilidad que m ocurra está dado por:

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle , \tag{C.6}$$

y el estado después de la medición será:

$$\frac{M_m |\psi\rangle}{\sqrt{p(m)}}. \tag{C.7}$$

En general los operadores de medición están dados por:

$$M_m = \sum_i \lambda_i |\psi\rangle \langle\psi| , \tag{C.8}$$

donde λ_i son sus autovalores y $|\psi\rangle$ es el estado a observar.

Cuando los estados son puros los operadores quedan como:

$$M_m = |\psi\rangle \langle\psi| . \tag{C.9}$$

Por otro lado, si el valor esperado de una variable (x) esta descrito por $E = \sum_x p(x)x$, donde $p(x)$ es la densidad de probabilidad. Entonces, el valor esperado para mediciones proyectivas están dadas por:

$$\begin{aligned} E(M) &= \sum_m p(m)m, \\ &= \sum_m m\langle\psi| P_m |\psi\rangle, \\ &= \langle\psi| \left(\sum_m mP_m \right) |\psi\rangle , \\ &= \langle\psi| (M) |\psi\rangle , \end{aligned} \tag{C.10}$$

donde P_m es el proyector sobre el espacio vectorial de M con autovalor m.

Cuarto postulado

El espacio de estados de un sistema compuesto es el producto tensorial entre los espacios de estados que componen el sistema.

Esto es, si tenemos sistemas numerados de 1 a n, entonces el estado conjunto $|\varphi\rangle$ estará descrito por:

$$|\varphi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle . \tag{C.11}$$

Apéndice D

Teorema de non-cloning

En este anexo se explica porque utilizando operadores de medición lineales, estados superpuestos no pueden ser clonados. Para explicar el teorema de no clonación consideraremos un experimento en polarización, donde se utilizará un perfecto dispositivo amplificador para clonar estados [5]. Este dispositivo debería tener el siguiente comportamiento:

$$|A_i\rangle |s\rangle = |A_s\rangle |ss\rangle , \tag{D.1}$$

donde $|A_i\rangle$ y $|A_s\rangle$ son los estados de entrada y salida del aparato, los cuales pueden no depender de la polarización. Los estados $|s\rangle$ y $|ss\rangle$ representan el estado de polarización y la clonación de éste (generando dos fotones). Al amplificar estados horizontal y vertical se tiene:

$$|A_i\rangle |0\rangle = |A_h\rangle |00\rangle , \tag{D.2}$$

$$|A_i\rangle |1\rangle = |A_v\rangle |11\rangle . \tag{D.3}$$

Un estado superpuesto generado en base a estados horizontal y vertical es un estado diagonal, el cual se representa como $|\psi_d\rangle = \alpha |0\rangle + \beta |1\rangle$ (si la polarización es 45^o entonces $\alpha^2 = \beta^2 = 1/\sqrt{2}$). La amplificación de un estado diagonal, estará dada por:

$$|A_i\rangle |\psi_d\rangle = |A_i\rangle (\alpha |0\rangle + \beta |1\rangle). \tag{D.4}$$

Considerando el postulado 3 de la MC (operador lineal), y las ecuaciones D.2 y D.3 se tiene:

$$|A_i\rangle |\psi_d\rangle = \alpha |A_i\rangle |0\rangle + \beta |A_i\rangle |1\rangle = \alpha |A_h\rangle |00\rangle + \beta |A_v\rangle |11\rangle . \tag{D.5}$$

Si los estados de los aparatos son idénticos ($|A_h\rangle = |A_v\rangle$), la ecuación D.5 se reescribe como:

$$|A_i\rangle |\psi_d\rangle = \alpha |00\rangle + \beta |11\rangle . \tag{D.6}$$

El resultado en (D.6) se obtiene con un operador lineal, sin embargo lo que el dispositivo debería generar es:

$$\begin{aligned} |A_i\rangle\,|\psi_d\rangle &= |A_d\rangle\,|\psi_d\rangle\,|\psi_d\rangle\,, \\ &= |A_d\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle), \\ &= |A_d\rangle\,(\alpha^2\,|0\rangle\,|0\rangle + \alpha\beta\,|0\rangle\,|1\rangle + \alpha\beta\,|1\rangle\,|0\rangle + \beta^2\,|1\rangle\,|1\rangle), \\ &= |A_d\rangle\,(\alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \alpha\beta\,|10\rangle + \beta^2\,|11\rangle). \end{aligned} \tag{D.7}$$

El resultado obtenido en D.7 es completamente diferente de D.6, esto debido a la imposibilidad de clonar estados superpuestos utilizando operadores lineales de medición [5]. Este argumento puede ser aplicada a cualquier tipo de sistema cuántico, el cual se diseñe sobre sistemas con propiedades superpuestas.

El teorema de non-cloning es uno de los resultados más tempranos de la información cuántica [42]. La posibilidad de transmitir estados con la seguridad de que estos no pueden ser clonados, permite utilizar esta aplicación en sistemas criptográficos permitiendo que la privacidad de comunicación sea protegida por las leyes de la MC.

Apéndice E

Potencia óptica sobre un interferómetro de Mach-Zehnder

En este Apéndice se estima un modelo de potencia óptica, a la salida de un interferómetro de Mach-Zehnder (MZ).

En la figura E.1 se muestra un interferómetro de MZ, éste es una configuración óptica aplicada a luz coherente la cual es dividida por dos caminos con largo distinto, para finalmente ser recombinados en la salida de la configuración [63, 64]. Si los haces divididos mantiene la condición de coherencia, el ser recombinados producirán una interferencia de salida, dependiente de la fase producto de la diferencia de camino. La fase o diferencia de camino, puede ser variada con elementos activos como un Piezo-eléctrico, tal como muestra la figura E.1, en cuyo caso la fase tendrá una dependencia en la tensión aplicada al elemento activo, la cual denominaremos fase de control $\delta_p(V)$.

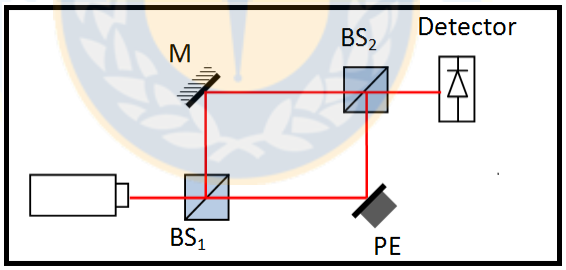


Figura E.1: MZI con fase controlada a través de un piezo-eléctrico. En la figura: (PE) piezo-eléctrico, (M) espejo, (BS) divisor de haz óptico.

La intensidad de salida de un láser I_0, puede escribirse como:

$$I_0 = Acos\left(w_0 t + \delta_0\right), \tag{E.1}$$

donde w_0 es dependiente de la longitud de onda λ, δ_0 es una fase global (la cual no afecta al sistema y puede ser despreciada, $\delta_0 = 0$), y A es la amplitud de potencia óptica.

Al incidir I_0 sobre el interferómetro, las intensidades por brazo después del divisor de haz (Beam Spliter, BS_1) serán:

$$\begin{aligned} I_f &= \frac{A}{2} cos(w_0 t + \delta_1), \\ I_c &= \frac{A}{2} cos(w_0 t + \delta_2 + \delta(V)), \end{aligned} \tag{E.2}$$

donde I_f e I_c corresponden a las intensidades sobre el camino con largo-fijo y largo-variable respectivamente, además δ_1 y δ_2 son fases iniciales producto de la diferencia de largo en los caminos ópticos. Como estas fases son fijas, tenemos que $\delta_{diff} = \delta_1 - \delta_2$, luego $\delta_2 = \delta_1 + \delta_{diff}$, esto es:

$$\begin{aligned} I_f &= \frac{A}{2} cos(w_0 t), \\ I_c &= \frac{A}{2} cos(w_0 t + \delta_{diff} + \delta_p(V)). \end{aligned} \tag{E.3}$$

Considerando $\delta(V) = \delta_{diff} + \delta_p(V)$ sobre (E.3), se tiene:

$$\begin{aligned} I_f &= \frac{A}{2} cos(w_0 t), \\ I_c &= \frac{A}{2} cos(w_0 t + \delta(V)). \end{aligned} \tag{E.4}$$

La recombinación de I_f e I_c en ambas salidas del BS_2, se escriben:

$$\begin{aligned} I_{out} &= \frac{1}{2} \left(I_f + I_c \right), \\ &= \frac{1}{2} \left[\frac{A}{2} cos(w_o t) + \frac{A}{2} cos(w_o t + \delta(V)) \right], \\ &= \frac{A}{4} \left[cos\left(w_o t + \frac{\delta(V)}{2} - \frac{\delta(V)}{2} \right) + cos\left(w_o t + \frac{\delta(V)}{2} + \frac{\delta(V)}{2} \right) \right]. \end{aligned} \tag{E.5}$$

Utilizando la identidad trigonométrica $cos(a \pm b) = cos(a)cos(b) \mp sen(a)sen(b)$ sobre la ecuación E.5 (donde $a = w_o t + \frac{\delta(V)}{2}$), se obtiene:

$$I_{out} = \frac{A}{4} \left[cos(w_o t + \frac{\delta(V)}{2}) \cdot cos(\frac{\delta(V)}{2}) \right]. \tag{E.6}$$

La potencia en el detector estará dada por $P = I_{RMS}^2$, entonces:

$$\begin{aligned} P = I_{RMS}^2 &= \frac{1}{T}\int_0^T \frac{A^2}{16}\left[cos(w_o t + \delta_0 + \frac{\delta(V)}{2})^2 \cdot cos(\frac{\delta(V)}{2})^2\right], \\ &= \frac{A^2}{2\pi 16} cos(\frac{\delta(V)}{2})^2 \int_0^{2\pi} \frac{1}{2}\left[1 + cos(2w_o t + 2\delta_0 + \delta(V)\right], \\ &= \frac{A^2}{32} cos(\frac{\delta(V)}{2})^2. \end{aligned} \tag{E.7}$$

El resultado mostrado en la ecuación E.7 nos muestra que la variación activa de fase sobre un interferómetro MZ ($\delta(V)$), produce una variación no lineal sobre la potencia óptica de salida, la cual podemos aproximar a:

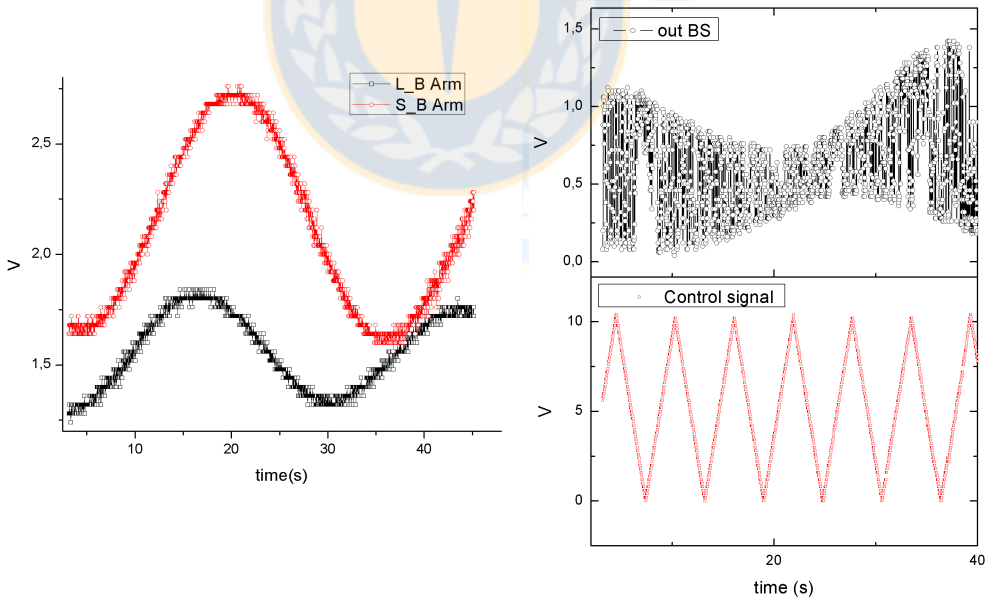
$$P \propto cos(\frac{\delta(V)}{2})^2 = \frac{1}{2}(1 + cos(\delta(V)). \tag{E.8}$$

Apéndice F

Potencia óptica sobre interferómetro MZ instalado en terreno

La potencia óptica de salida en un interferómetro-MZ (MZI) instalado en terreno, estará afectada por variaciones propias de las condiciones ambientales del enlace. Por esto, el modelo canónico no es válido, y se requiere modelar la potencia de salida considerando los parámetros ambientales mencionados.

La figura F.1.a muestra las variaciones empíricas en los brazos de un MZI instalado en terreno. Las perturbaciones mostradas son propias de las condiciones ambientales, dado un enlace con $3{,}7km$ de fibra óptica instalada sobre la Universidad de Concepción. La recombinación de salida se muestra en la figura F.1.b, en ésta se aprecia como la potencia óptica es variable en el tiempo.



(a) (b)

Figura F.1: Detección de señal de control sobre el fotodetector p-i-n fibra montada en terreno. a)Intensidad por brazo, señal de control constante. b) Intensidad en la salida del BS de Bob, señal de control variable.

Con las mediciones mostrada en la figura F.1.a podemos modelar las intensidades por brazo I_{SB} e I_{LB}, contemplando una variación aditiva y proporcional. Con estos parámetros, las intensidades por brazo del MZI, quedan como:

$$\begin{aligned} I_{SB} &= \beta_S cos(w_S t)\frac{A}{2}cos(w_c t) + b_S(t), \\ I_{LB} &= \beta_L cos(w_L t)\frac{A}{2}cos(w_c t + \delta(V)) + b_L(t), \end{aligned} \tag{F.1}$$

donde las frecuencias, amplitudes y offset de oscilación en la distorsión son independientes por brazo ($w_S \neq w_L$, $\beta_S \neq \beta_L$ y $b_S(t) \neq b_L(t)$). Por otro lado, $Acos(w_c t + \phi_c)$ corresponde al haz de control. La recombinación de los haces en un BS, queda como:

$$\begin{aligned} I_{out} &= I_{SB} + I_{LB}, \\ I_{out} &= \beta_S cos(w_S t)\frac{A}{2}cos(w_c t) + b_S(t), \\ &\quad + \beta_L cos(w_L t)\frac{A}{2}cos(w_c t + \delta(V)) + b_L(t). \end{aligned} \tag{F.2}$$

Utilizando identidades trigonométricas en la ecuación F.2, se obtiene:

$$\begin{aligned} I_{out} &= \beta_S cos(w_S t)\frac{A}{2}[cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2}) + sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})] \\ &\quad + \beta_L cos(w_L t)\frac{A}{2}[cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2}) - sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})] \\ &\quad + b_S(t) + b_L(t), \\ &= \frac{A}{2}[\beta_S cos(w_S t) + \beta_L cos(w_L t)][cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2})] \\ &\quad + \frac{A}{2}[\beta_S cos(w_S t) - \beta_L cos(w_L t)][sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})] \\ &\quad + b_S(t) + b_L(t). \end{aligned} \tag{F.3}$$

Reemplazando $\alpha_1 = \frac{A}{2}[\beta_S cos(w_S t) + \beta_L cos(w_L t)]$, $\alpha_2 = \frac{A}{2}[\beta_S cos(w_S t) - \beta_L cos(w_L t)]$ y $\alpha_3 = b_S(t) + b_L(t)$ en la ecuación F.3, se obtiene:

$$\begin{aligned} I_{out} &= \alpha_1[cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2})] \\ &+ \alpha_2[sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})] \\ &+ \alpha_3, \\ &= \alpha_1 f_1 + \alpha_2 f_2 + \alpha_3. \end{aligned} \tag{F.4}$$

El cuadrado de la intensidad en (F.4), es de la forma:

$$\begin{aligned} I_{out}^2 &= (\alpha_1 f_1 + \alpha_2 f_2 + \alpha_3)^2, \\ &= \alpha_1^2 f_1^2 + 2\alpha_1 f_1(\alpha_2 f_2 + \alpha_3) + (\alpha_2 f_2 + \alpha_3)^2, \\ &= \alpha_1^2 f_1^2 + 2\alpha_1\alpha_2 f_1 f_2 + 2\alpha_1\alpha_3 f_1 + \alpha_2^2 f_2^2 + 2\alpha_2\alpha_3 f_2 + \alpha_3^2. \end{aligned} \tag{F.5}$$

Como la potencia óptica a observar es de la forma $P = I_{RMS}^2$, se tiene:

$$I_{RMS}^2 = \frac{1}{2\pi}\int_0^{2\pi} (\alpha_1^2 f_1^2 + 2\alpha_1\alpha_2 f_1 f_2 + 2\alpha_1\alpha_3 f_1 + \alpha_2^2 f_2^2 + 2\alpha_2\alpha_3 f_2 + \alpha_3^2) dw_c t. \tag{F.6}$$

Las soluciones para cada expresión son de la forma:

$$\begin{aligned} \int_0^{2\pi} \alpha_1^2 f_1^2 dw_c t &= \int_0^{2\pi} \alpha_1^2 (cos(w_c t + \frac{\delta(V)}{2})^2 cos(\frac{\delta(V)}{2})^2) dw_c t, \\ &= 2\pi\alpha_1^2 cos(\frac{\delta(V)}{2})^2). \end{aligned} \tag{F.7}$$

$$\begin{aligned}
&\int_0^{2\pi} 2\alpha_1\alpha_2 f_1 f_2 dw_c t = \\
&\int_0^{2\pi} 2\alpha_1\alpha_2[cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2})][sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})]dw_c t, \\
&= \int_0^{2\pi} 2\alpha_1\alpha_2[sen(w_c t + \frac{\delta(V)}{2})cos(w_c t + \frac{\delta(V)}{2})]sen[\frac{\delta(V)}{2})cos(\frac{\delta(V)}{2})]dw_c t, \\
&= \int_0^{2\pi} \frac{1}{2}\alpha_1\alpha_2[sen(2w_c t + \delta(V))sen(\delta(V))]dw_c t, \\
&= 0.
\end{aligned} \tag{F.8}$$

$$\begin{aligned}
\int_0^{2\pi} 2\alpha_1\alpha_3 f_1 dw_c t &= \int_0^{2\pi} 2\alpha_1\alpha_2[cos(w_c t + \frac{\delta(V)}{2})cos(\frac{\delta(V)}{2})]dw_c t, \\
&= 0.
\end{aligned} \tag{F.9}$$

$$\begin{aligned}
\int_0^{2\pi} \alpha_2^2 f_2^2 &= \int_0^{2\pi} \alpha_2^2[sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})]dw_c t, \\
&= 2\pi\alpha_2^2 sen(\frac{\delta(V)}{2})^2.
\end{aligned} \tag{F.10}$$

$$\begin{aligned}
\int_0^{2\pi} 2\alpha_2\alpha_3 f_2 dw_c t &= \int_0^{2\pi} 2\alpha_2\alpha_3[sen(w_c t + \frac{\delta(V)}{2})sen(\frac{\delta(V)}{2})]dw_c t, \\
&= 0.
\end{aligned} \tag{F.11}$$

$$\int_0^{2\pi} \alpha_3^2 = 2\pi\alpha_3^2. \tag{F.12}$$

Utilizando los resultados de (F.7), (F.8), (F.9), (F.10), (F.11) y (F.12) sobre la ecuación F.6, se obtiene:

$$\begin{aligned} I_{RMS}^2 &= \alpha_1^2 cos(\frac{\delta(V)}{2})^2 + \alpha_2^2 sen(\frac{\delta(V)}{2})^2 + \alpha_3^2, \\ &= \alpha_1^2 cos(\frac{\delta(V)}{2})^2 + \alpha_2^2[1 - cos(\frac{\delta(V)}{2})^2] + \alpha_3^2, \\ &= (\alpha_1^2 - \alpha_2^2) cos(\frac{\delta(V)}{2})^2 + \alpha_2^2 + \alpha_3^2. \end{aligned} \tag{F.13}$$

Para simplificar la expresión de la ecuación F.13, definimos un contraste temporal de la forma $c(t) = \alpha_1^2 - \alpha_2^2$ y un offset $b(t) = \alpha_2^2 + \alpha_3^2$, ambas variaciones con frecuencias lentas ($\propto 27Hz$). Finalmente la potencia óptica de salida en nuestro MZI, se puede aproximar de la forma:

$$P \propto c(t) cos(\frac{\delta(V)}{2})^2 + b(t). \tag{F.14}$$