UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE FÍSICA

"INTRODUCCIÓN A LA CRIPTOGRAFÍA CUÁNTICA EXPERIMENTAL: DISTRIBUCIÓN DE UNA CLAVE CUÁNTICA POR AIRE LIBRE"

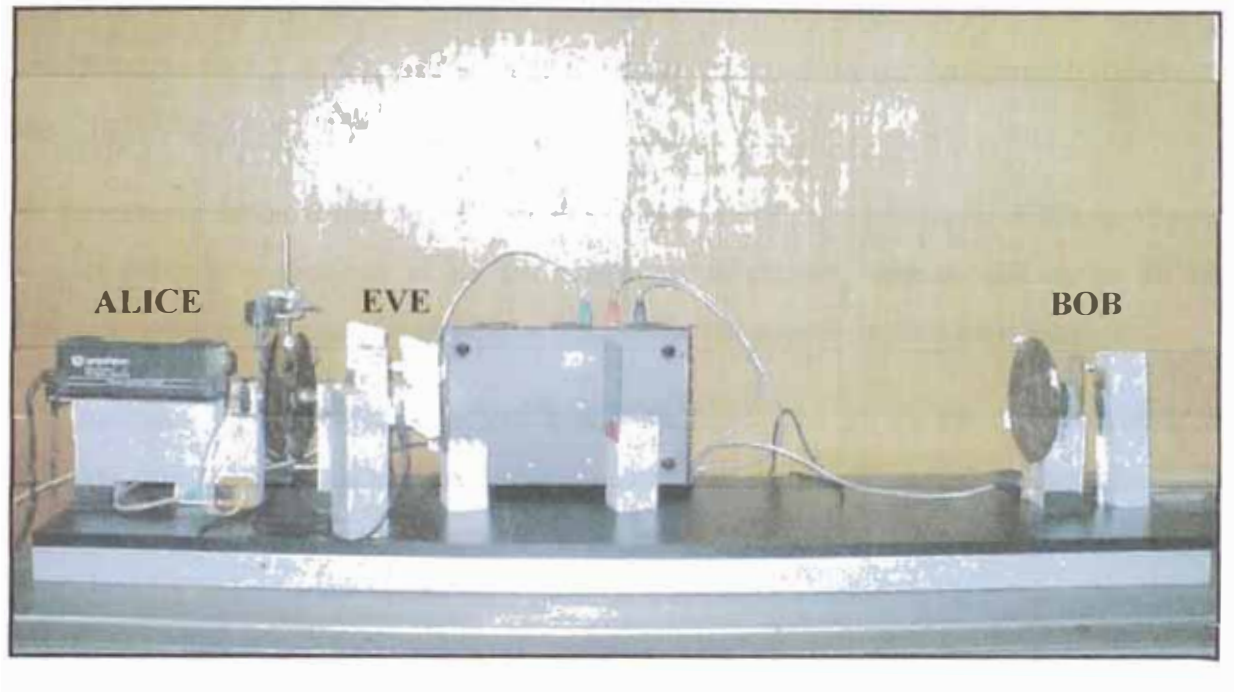
TESIS
PARA OPTAR EL TÍTULO PROFESIONAL DE LICENCIADO EN FÍSICA

CARLOS MANUEL DÍAZ DOMÍNGUEZ

Enero 2010
LIMA-PERÚ

CONTENIDO

"Introducción a la Criptografía Cuántica Experimental: Distribución de Clave Cuántica por aire libre"



Según el diccionario de la Real Academia Española:

***Criptografía**. (Del griego kryptós "oculto" y graphein "escritura"). Arte de escribir con clave secreta o de un modo enigmático.*

Resumen

Este trabajo trata de la Criptografía Cuántica, una de las aplicaciones prácticas de la fascinante "Computación Cuántica", que mas avance tecnológico viene mostrando hasta la fecha.

Como un primer trabajo de introducción a la criptografía cuántica en nuestro medio, se ha modelado en computadora clásica y construido experimentalmente una máquina básica de criptografía capaz de enviar una clave "secreta" mediante pulsos de fotones a una distancia de 1.5 m, a través del aire libre, utilizando el protocolo cuántico BB84 y el algoritmo One-Time Pad.

Es importante destacar que aunque nuestra máquina utiliza el protocolo BB84, su diseño es simplificado y distinto al de las máquinas modernas, diseño que surge de las limitaciones económicas que obligan a utilizar partes ópticas mucho más simples.

Los métodos de criptografía actual basan su seguridad en la enorme cantidad de cálculos que tendría que realizar una computadora moderna para descifrar claves de seguridad que en promedio tomaría años en lograrlo. Por el contrario una futura computadora cuántica realizaría esos mismos cálculos en cuestión de minutos haciendo vulnerables todos los métodos criptográficos actuales Por ello, en la actualidad, se desarrollan nuevos métodos de criptografía que sean intrínsecamente invulnerables aún frente a una computadora cuántica.

Antes de construir la máquina criptográfica se dedujo fórmulas teóricas que predicen el comportamiento estadístico de la transmisión de bits en presencia de ruido y espía Luego se elaboró un programa de simulación de la generación de la clave "secreta" escrito en el lenguaje de programación Microsoft Visual C#.

Luego de las simulaciones computarizadas, se construyó la máquina básica de criptografía, la misma que consta de las siguientes partes:

- La parte óptica que está constituida por un laser He-Ne polarizado de 1mW, un atenuador de potencia manual, un "chopper", un conjunto de polarizadores fundamentalmente para codificar y medir la señal, un montaje en base a vidrios que actúan como separadores de haz y fototransistores para detectar la señal.

- La parte electro-mecánica está constituida por un conjunto de motores a paso y por fototransistores ambos controlados por circuitos integrados que forman una interfaz paralela conectada a una PC. El software de control de esta parte electro-mecánica implementa además el protocolo BB84.

Con la máquina construida se realizaron tres experimentos:

- El objetivo primario de la presente tesis es la generación de una clave privada por aire utilizando el protocolo cuántico BB84. Los resultados muestran una coincidencia con las predicciones teóricas y con las simulaciones mediante el software desarrollado, es decir hubo una coincidencia entre las longitudes de las claves previstas (teóricas y simuladas) y la experimental

- Se implemento el método de interceptación denominado Photon Number Splitting (PNS) que consiste en que el espía desvía parte de los fotones. Este ataque es efectivo cuando el pulso contiene varios fotones como es nuestro caso. En estas condiciones se muestra que el espía obtiene la clave sin que el emisor o receptor se den cuenta de ello. Sin embargo cuando se atenúa la intensidad del haz láser el espía tiene dificultades en obtener la clave, incluso se ha podido determinar experimentalmente la existencia de un mínimo de intensidad de haz mediante el cual se logra evitar que el espía obtenga alguna información, permitiendo todavía que emisor y receptor construyan una clave segura.

- Finalmente se utilizó la máquina para enviar mensajes encriptados. Este proceso es sencillo pero muestra la flexibilidad de la máquina que puede ser usado para generar una clave privada y luego enviar el mensaje encriptado.

Introducción

La importancia y necesidad de la criptografía cuántica radica en que las investigaciones actuales hacen suponer que en unos 20 años estarán en funcionamiento las primeras computadoras cuánticas y en alrededor de 30 años ya serian de uso común (2) Estas computadoras podrán desencriptar las claves más seguras que se usan actualmente en Internet, bancos y grandes empresas. Incluso ya existen algoritmos cuánticos capaces en principio de realizar dicha desencriptación como el algoritmo de Shor (3) y el de las Sumas Gauss (4) .

Los métodos de encriptación actuales basan su seguridad en la dificultad de las computadoras modernas de realizar enormes cálculos matemáticos y por tanto son vulnerables a ataques por espías con suficiente potencia de cálculo. En contraste existe una posibilidad en la que la seguridad, en el límite es incondicional y está garantizada por leyes fundamentales de la Física Cuántica. En el límite esta posibilidad incluso es invulnerable ante una computadora cuántica.

Las primeras ideas de lo que ahora se conoce como Computación Cuántica aparecieron en 1981 durante la "*Primera Conferencia sobre la Física y Computación*", organizada por el Instituto Tecnológico de Massachusetts (MIT), donde Richard Feynman (1918-1988) observó que las computadoras convencionales se hacían muy lentas al simular la evolución de sistemas cuánticos y sugirio que sólo una computadora construida en base a principios cuánticos podrá ser capaz de realizar dichas simulaciones (5) Feynman describió un "Simulador Cuántico Universal" que emulaba el comportamiento de cualquier sistema físico, pero no fue hasta 1985 cuando David Deutsch propuso la primera máquina de Turing Cuántica[13] con la que se establecieron las bases para el desarrollo de una computadora cuántica. Desde esa fecha se han desarrollado algoritmos teóricos cuánticos capaces de resolver problemas que son imposibles o muy difíciles para las computadoras actuales Entre los más conocidos están el algoritmo de Shor (3) (1994) que factoriza[14] números enteros, el algoritmo de Grover (6) (1996) que realiza una búsqueda rápida en una base de datos desordenada y los más recientes el algoritmo

[13] La máquina de Turing clásica es un modelo matemático de un dispositivo de cálculo, se propuso en 1936, y es capaz de realizar teóricamente cualquier cálculo matemático. Es la base del diseño de las computadoras actuales. La máquina de Turing Cuántica es similar a la clásica con la única diferencia que en vez de usar un bit utiliza un bit cuántico. En el Apéndice A se compara estas dos máquinas.
[14] Factorizar un número consiste en descomponerlo en sus factores primos.

de las Sumas de Gauss (4) que factoriza números enteros en el 2006 y el algoritmo para resolver sistemas de ecuaciones lineales (7) en el 2008.

Sin embargo, la construcción física de una computadora cuántica que implemente estos algoritmos con los qubits[15] necesarios todavía es muy complicado[16]. El principal problema es que la tecnología actual aún no permite construir el hardware necesario para controlar totalmente la interacción de un estado cuántico con su entorno, lo que se conoce como el problema de la decoherencia.

Uno de los productos de la computación cuántica que ha alcanzado un gran desarrollo es la Criptografía Cuántica, a la cual está dedicada esta tesis.

En la Figura 1 se muestra a Richard Hughes (8) enviando por el aire fotones polarizados a una distancia de 10 Km desde su laboratorio (circunferencia roja) hacia las montañas.

Figura 1: Distribución de una clave cuántica por aire libre utilizando el protocolo BB84. El experimento fue realizado en Los Álamos, Nuevo Mexico en el 2002.

[15] El qubit (Quantum Bit) o bit cuántico es el equivalente cuántico del bit clásico. Más detalles del qubit y la Computación Cuántica se encuentra en el Apéndice A.

[16] En 1998, Jonathan A. Jones y Michele Mosca de la Universidad de Oxford construyeron la primera computadora cuántica de 2 qubits utilizando NMR. ese mismo año Isaac Chuang (IBM). Neil Gerschenfeld (MIT) y Mark Kubinec (Universidad de Stanford) También construyeron independientemente una computadora cuántica de 2 qubits NMR. En el 2000 la Universidad Técnica de Munich presentó una computadora cuántica de 5 qubits NMR. En el 2001 IBM presentó una computadora cuántica de 7 qubits NMR. En el 2006 el Instituto Cuántico de Waterloo junto al MIT lograron un computadora cuántico de 12 qubits NMR (54). Y en el 2009 Robert Schoelkopf, Steven Girvin y Leonardo DiCarlo de la Universidad de Yale presentaron el primer procesador cuántico de 2 qubits basado en semiconductores (56).

El primer protocolo de distribucion de una clave cuántica fue propuesto por Bennett y Brassard en 1984 (9) y la primera transmisión de señales cuánticas fue realizada por Bennet y Brassard en los laboratorios de IBM en octubre de 1989 (10) a una distancia de 32 cm. (Figura 2).

Figura 2: Máquina construida por Bennet y Brassard en los laboratorios de IBM en 1989. El equipo consta básicamente de 3 partes: el emisor de fotones (Alice), el canal cuántico (espacio por donde viajan los fotones) y el receptor de fotones (Bob).

El record actual de distancia transmitida se logro en el 2007, donde científicos europeos transmitieron una clave cuántica por aire a una distancia de 144 Km (Figura 3), utilizando el protocolo BB84 (11) y luego utilizando fotones entrelazados utilizando el protocolo E91 (12). El objetivo futuro y necesario es realizar transmisiones seguras a satélites que se encuentran a una distancia entre 300 y 500 Km Y en este año 2009, los mismos científicos han batido un nuevo record al teletransportar fotones entre ambas islas, 144 Km.

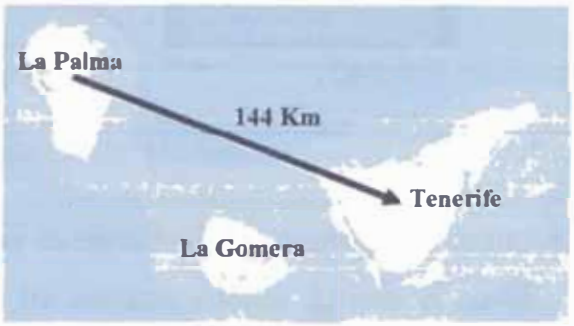


Figura 3: Los fotones se enviaron por aire desde la isla La Palma hacia la isla Tenerife en España. Para ello se utilizo como receptor uno de los telescopios de la Agencia Espacial Europea en la isla Tenerife.

Una de las organizaciones de la criptografía cuántica a nivel internacional es la red DARPA[17] Quantum Network en la que participan BBN Technologies, QinetiQ y las Universidades de Harvard y Boston. Está red está construida en base a fibra óptica y

[17] Defense Advanced Research Projects Agency (www.darpa.mil).

utiliza criptografía cuántica para proteger las comunicaciones intercambiadas, funciona desde el 2004 en Massachusets (13).

Así mismo existen empresas como la Id Quantique[18] que comercializan sistemas de criptografía cuántica a través de fibra óptica. Su más reciente producto el **id3110 Clavis2** (14) transmite con seguridad hasta 50 Km. con una velocidad de 1000 bits/s utiliza el protocolo BB84 y su costo es de alrededor de US $ 200 mil (Figura 4).

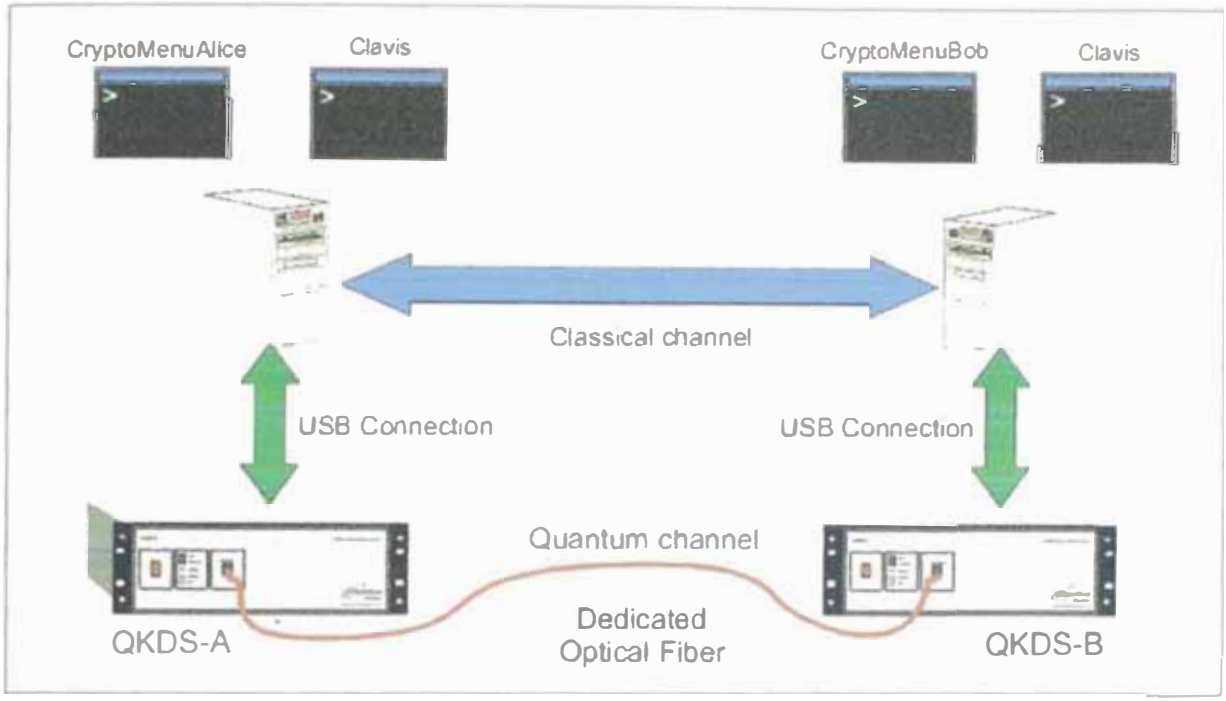


Figura 4: Configuración del modelo id3110 Clavis.

El 21 de octubre del 2007, esta empresa, utilizó su tecnología en criptografía cuántica para generar claves de encriptación y asegurar las comunicaciones durante el envió y conteo de votos en elecciones del parlamento del Cantón de Ginebra en Suiza (14).

Actualmente se observa un gran crecimiento de este tipo de tecnología en numerosos sectores de la sociedad donde la seguridad es un requisito crítico. Cada vez más empresas gastan recursos y poseen programas de investigación en sistemas de seguridad basados en criptografía cuántica como HP, IBM, Toshiba, Mitsubishi, Siemens, ARC (Austrian Research Center), NEC y NTT (Nippon Telegraph and Telephone de Japón) (13), Id Quantique, MagiQ, SmartQuantum, AT&T, Nokia, Nortel Networks, BBN Technologies, Fujitsu, QinetiQ, NIST, DARPA (15).

[18] Fundada en el 2001 por los físicos Nicolas Gisin, Grégoire Ribordy, Olivier Guinnard y Hugo Zbinden de la Universidad de Ginebra en Suiza (www.idquantique.com). Otras empresas son MagiQ Technologies en New York (www.magiqtech com) y SmartQuantum en Francia (www smartquantum.com).

Y desde el 2008 se desarrolla en España un prototipo de red metropolitana de criptografía cuántica que estaría disponible en el 2010 para ser implantada en cualquier red urbana de telecomunicaciones. El prototipo se desarrolla en el marco del Proyecto de Investigación y Desarrollo (www.cenitsegura.com), integrado por un Consorcio de doce empresas y quince Organismos Públicos de Investigación, liderados por Telefónica Investigación y Desarrollo El equipo está constituido por investigadores integrado por físicos, informáticos, ingenieros de telecomunicación y matemáticos de la Universidad Politécnica de Madrid. El proyecto tiene un presupuesto de 31 millones de euros y se basa en la red SECOQC[19] ya operativa en Viena[20]. La finalidad de este proyecto es dar soluciones de seguridad integrales, capaces de hacer frente a las actuales amenazas a la seguridad en las telecomunicaciones que presentan las redes convencionales. Los fundamentos de este trabajo fueron presentados el 8 de octubre del 2008 en Viena en la conferencia SECOQC sobre redes cuánticas. Citando lo dicho en la conferencia "*Una nueva tecnología está protagonizando una importante revolución en el campo de la criptografía. Basado en los principios de la física cuántica, el intercambio cuántico de claves proporciona el método más seguro conocido de intercambio de claves para cualquier método de cifrado de información. Y, por encima de todo, es una tecnología que es segura ahora y lo será en el futuro*".

[19] SECOQC (Secure Communication based on Quantum Cryptography. www secoqc.net) es un proyecto europeo que agrupa universidades y empresas de ese continente que investigan y desarrollan la Criptografía Cuántica con el objetivo de enfrentar futuras amenazas de interceptación tecnológica en las comunicaciones y obtener una ventaja económica europea.

[20] Es una red que consta de 7 enlaces ópticos de una longitud de entre 6 y 82 Km, 6 de ellos sobre fibra óptica y un enlace al aire. Los socios del proyecto demostraron en el congreso SECOQC del 2008 que el sistema funcionaba correctamente en la generación y distribución de claves en toda la red. la detección de intrusos y otras prestaciones de la red. Este proyecto inicio sus investigaciones desde abril del 2004.

Estructura de la Tesis

La tesis está compuesta de tres partes: Fundamento teórico (Capítulos 1 y 2), trabajo experimental (Capítulos 3 al 9) y 4 apéndices.

El capitulo 1 trata de la Criptografía Clásica, en la que definimos los conceptos más importantes y terminología utilizada Se hace una diferencia entre clave privada y pública, se explica porque se prefiere la clave pública. Se describe con detalle el algoritmo RSA y se muestra un ejemplo de su utilización. Al terminar se menciona brevemente otros protocolos clásicos.

El capitulo 2 trata de la Criptografía Cuántica, en la que se examina la vulnerabilidad de los algoritmos clásicos y se analiza con detalle uno de los algoritmos cuánticos que rompería la seguridad de los algoritmos actuales en una hipotética computadora cuántica: el algoritmo de Shor y también se describe con detalle una posible solución al problema futuro de la seguridad de la comunicación: el protocolo cuántico BB84. En este análisis se incluye el error en la transmisión de datos producidos por la presencia de ruido y la intervención de un espía. Para demostrar que el protocolo es seguro se deducen varias fórmulas probabilísticas para cada caso.

Para presentar el trabajo experimental (simulación en computadora y construcción de un equipo de criptografía) el Capítulo 3 presenta algunas tesis recientes que tratan el tema de la criptografía cuántica realizando una transmisión de fotones tanto por aire libre como por fibra óptica y utilizando preferentemente el protocolo BB84.

En el Capítulo 4 se deduce las relaciones probabilísticas en la transmisión de la clave para la máquina que construimos Se describe como adaptándonos a los escasos recursos económicos, se construyó una máquina sencilla pero que en el límite revela aspectos del comportamiento cuántico. Se tuvo que reemplazar componentes importantes como separadores de haces o beamsplitters (polarizantes y no polarizantes) por discos polarizadores con motores a paso y fuentes de fotones individuales por pulsos de fotones, además se dejo de usar varios elementos como laminas retardadoras media onda, lentes, filtros, etc. Esto convirtió a nuestra máquina en algo que funciona diferente pero que mostramos da los mismos resultados que una máquina correcta, pues se analizo con detalle cada caso de transmisión de la clave, incluyendo ruido y espía. Obteniendo las mismas fórmulas probabilísticas de la máquina moderna completa.

El Capítulo 5 muestra las simulaciones de la máquina que se construyó en el límite cuando se puede decir que es cuántica (fotones individuales). Aquí se comprueba todas las fórmulas obtenidas en el Capítulo 4 y se realiza gráficos que muestran la naturaleza probabilística del experimento. Los programas de simulación fueron realizados en Microsoft Visual C#.

El Capitulo 6 describe cada parte de los componentes de la máquina construida comparándolas con una máquina moderna. Se muestra las configuraciones utilizadas para la transmisión de la clave, primero sin espía y sin ruido y luego con espía usando el método de ataque Photon Number Splitting (PNS).

El Capitulo 7 muestra la realización del experimento y resultados obtenidos, explicando con detalle cada paso de la transmisión de la clave sin espía y sin ruido y luego la transmisión con un espía que usa el método de ataque PNS. Además se muestra como utilizar la máquina para transmitir el mensaje encriptado

El Capítulo 8 sugiere un posible proyecto futuro que estamos en la capacidad de ejecutar pues el único inconveniente es el económico, esta propuesta consiste en construir una máquina realmente cuántica e iniciar investigaciones en computación cuántica experimental y teleportación cuántica de fotones.

El Capítulo 9 compila todas las conclusiones de la tesis: las del cálculo probabilístico en la transmisión de la clave, de la simulación computarizada y del experimento con la máquina.

Finalmente se tiene 4 apéndices que desarrollan un conjunto de temas que sirven de soporte a algunos conceptos utilizados en la tesis, entre los más importantes tenemos una introducción a la Computación Cuántica, descripción de otros protocolo cuánticos, estadística de fotones, una demostración experimental de que el fotón se comporta como una partícula cuando pasa por un beamsplitter, cambio de polarización en la reflexión y refracción de la luz en sistema de vidrios, los códigos de programación tanto de la simulación como del software de control de la máquina, etc.

PARTE I

FUNDAMENTO TEÓRICO

Esta Parte I consta de dos Capítulos. En el Capitulo 1 se explica la terminología y las características de la Criptografía Clásica y, se analiza también el algoritmo actualmente más utilizado en este campo, diseñado en 1978 por Ronalt Rivest, Adi Shamir y Leonar Adleman (RSA). El Capitulo 2 está dedicado a introducir la Criptografía Cuántica y comienza con la descripción del algoritmo cuántico de Shor que rompe la seguridad de la criptografía clásica. Luego se muestra con detalle el protocolo cuántico más popular, desarrollado en 1982 por Bennet y Brassar (BB84), deduciendo cada fórmula probabilística de acierto y error en la generación de la clave secreta incluyendo los efectos del ruido presente en el sistema y eventuales ataques de interceptación de un espía.

Capítulo 1

Criptografía Clásica

Según el diccionario de la Real Academia Española, ***criptografía*** es el arte de escribir con clave secreta o de un modo enigmático. Es interesante revisar algunas definiciones:

La ***criptología*** (del griego *kryptós* "oculto" y *lógos* "palabra") es el arte de encriptar y desencriptar mensajes, está formada por la ***criptografía*** y el ***criptoanálisis***.

La ***criptografía*** (del griego *kryptós* "oculto" y *graphein* "escritura") es el arte de encriptar un mensaje y desencriptarlo usando una clave.

El ***criptoanálisis*** (del griego kryptós "oculto" y analýein "desamarrar") es el arte de desencriptar un mensaje encriptado sin conocer la clave.

La criptografía es tan antigua como la civilización, diversas razones militares, políticas, religiosas o comerciales impulsaron desde tiempos remotos el uso de las escrituras secretas.

El primer uso de tipo militar constatado es en la guerra entre Esparta y Atenas en el siglo V a.C. El encriptado consistía en la introducción de símbolos innecesarios que desaparecían al enrollar el mensaje en un rodillo llamado "escítalo espartano" de longitud y grosor determinados. En el siglo I a.C., Julio César utilizó un método que consistía en sustituir cada letra por la que ocupaba cierto número de posiciones más adelante en el abecedario.

En la Edad Media, San Bernardino evitaba la regularidad de los signos y conseguía que el criptoanálisis por el método de frecuencia[21] no fuese efectivo. Utilizaba un signo para cada consonante, tres distintos para cada vocal e intercalaba símbolos sin sentido.

El primer libro del que se tiene constancia sobre el tema es el "LiberZifrorum" de Cicco Simoneta en el siglo XIV. En 1466 León Battista Alberti, considerado por muchos como el padre de la criptología, crea la primera máquina de criptografía consistente en dos círculos concéntricos, que giran independientes consiguiendo cada una un alfabeto

[21] El análisis de frecuencia consiste en buscar signos que tengan similar frecuencia al de una letra del alfabeto. Por ejemplo, en un texto extenso en español la letra "E" aparece un 16.78%, la "A" 11.96%, la "O" 8.69%, la "L" 8.37%, la "S" 7.88%, la "N" 7.01%, la "D" 6.87%, la "R" 4.94%, la "U" 4.80%, etc.

de transposición. En el siglo XVI Girolamo Cardano empleó una tarjeta perforada que debía colocarse sobre el texto para poder leerlo. En el mismo siglo el francés Viete descifró los mensajes encriptados de Felipe II, siendo así uno de los primeros criptoanalistas con éxito de la historia. Del mismo siglo es la obra "Traité des Chiffres" del francés Blaise de Vigenére en el que contaba todas las técnicas empleadas en su tiempo. Otras técnicas a contar son las empleadas por Carlos I de Inglaterra que en el siglo XVII empleó códigos de sustitución silábica y Napoleón que empleó el método Richelieu y Rossignol que consistía en asignar números a grupos de una o más letras.

En el siglo XIX se usó masivamente el método de transposición consistente en la reordenación según distintos criterios. Kerckhoffs escribe el libro "La criptografía militar" en el que cuenta las normas que debe cumplir un buen sistema criptográfico.

En la I Guerra Mundial los alemanes emplearon el método ADFGX que consistía en convertir las distintas letras del mensaje en un par de otras letras, conforme una tabla encabezada, a izquierda y encima, por ADFGX y que contenía en su interior una mezcla aleatoria de todos los caracteres del alfabeto utilizado Por ejemplo:

	A	D	F	G	X
A	v	g	z	p	l
D	b	k	r	f	u
F	o	h	e	t	a
G	d	w	m	x	q
X	n	y	s	ij	c

Si se desea enviar el mensaje "atacar por el sur", la "a" se transforma en "FX" (fila y columna de la tabla), la "t" se convierte en "FG", etc.

Para complicar más aún este cifrado se mezclaba con una palabra clave cualquiera que obviamente sólo debían conocer el emisor y el receptor Sin embargo el criptoanalista Georges Jean Pain de la inteligencia francesa rompió la seguridad del ADFX contribuyendo a la derrota alemana.

En el periodo entre guerras la criptología tuvo un gran avance debido a la necesidad de vías seguras de comunicación diplomática.

En la II Guerra Mundial los alemanes usaban la máquina Enigma, mientras que los norteamericanos empleaban el código navajo que utilizaba como base el dialecto de los indios navajos.

1.1 Terminología estandarizada de la Criptografía Clásica

Se tiene la siguiente situación: El emisor A (llamado Alice) desea enviar un mensaje al receptor B (llamado Bob) a través de una conexión segura. Un espía E (llamado Eve) que obtiene el mensaje no debe ser capaz de obtener información de él. En la Figura 5 se muestra un envió sin encriptar, cualquier espía que interviene el mensaje lo descubre con facilidad.

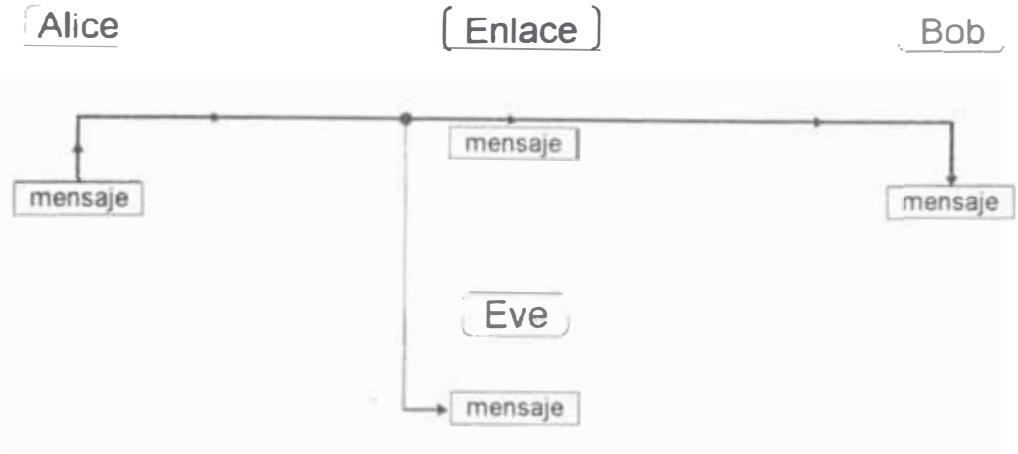


Figura 5: Alice envía un mensaje sin encriptar a Bob, Eve lo intercepta y lee el mensaje sin dificultad.

Como se observa en la Figura 5, Alice no puede enviar un ***texto en claro***[22] a Bob por causa de Eve, Alice tiene que transformar el texto en claro en algo ilegible para Eve, pero que Bob lo descifrará usando una clave.

1.1.1 Encriptación y desencriptación

Alice escribe un texto en claro y lo transforma con el objetivo de ocultar la información, esto se llama ***encriptación***.

Cuando Bob recibe el mensaje encriptado aplica una clave para regresar el mensaje a texto en claro. Esto se llama ***desencriptación***. En la Figura 6 se muestra este proceso Alice encripta el texto en claro y envía el texto encriptado a Bob quien puede desencriptarlo obteniendo nuevamente el texto en claro.

[22] Se denomina ***texto en claro*** al mensaje escrito de manera legible, que se puede leer y entender.

En cambio Eve, que intercepta el mensaje encriptado, no puede descifrarlo pues desconoce la clave de desencriptación.

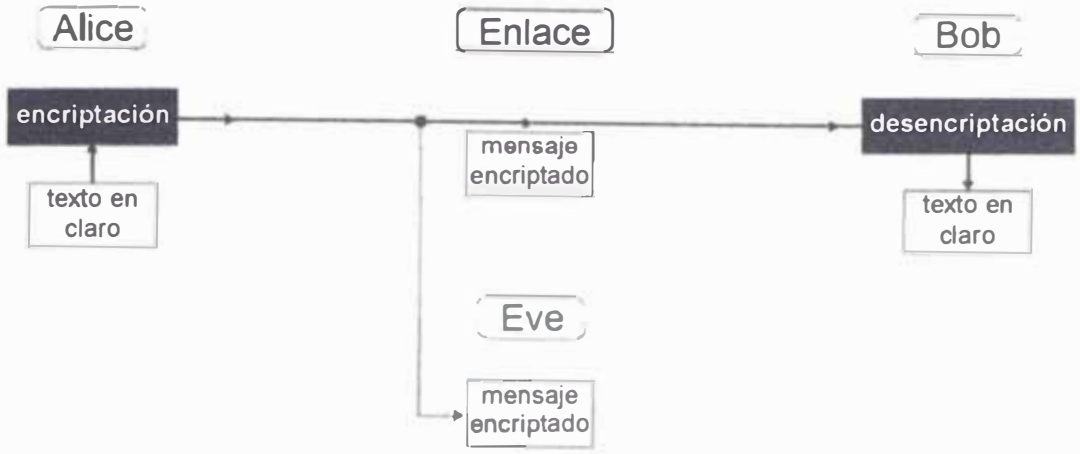


Figura 6: Alice envía un mensaje encriptado a Bob, Eve lo intercepta y no puede descifrarlo, pero Bob si lo descifra pues conoce la clave de encriptación.

1.1.2 Algoritmos de criptografía. Claves de encriptación y desencriptación

El procedimiento usado para encriptar y desencriptar el mensaje es llamado ***algoritmo de criptografía***. Generalmente hay dos algoritmos uno de encriptación y otro de desencriptación. La ***clave*** viene a ser una secuencia alfanumérica que se utiliza para encriptar o desencriptar mensajes. El algoritmo de encriptación aplica la clave de encriptación al mensaje en claro para obtener un mensaje encriptado. El algoritmo de desencriptación aplica la clave de desencriptación al mensaje encriptado para obtener el mensaje en claro. En la Figura 7, se muestra el diagrama final de la criptografía clásica.

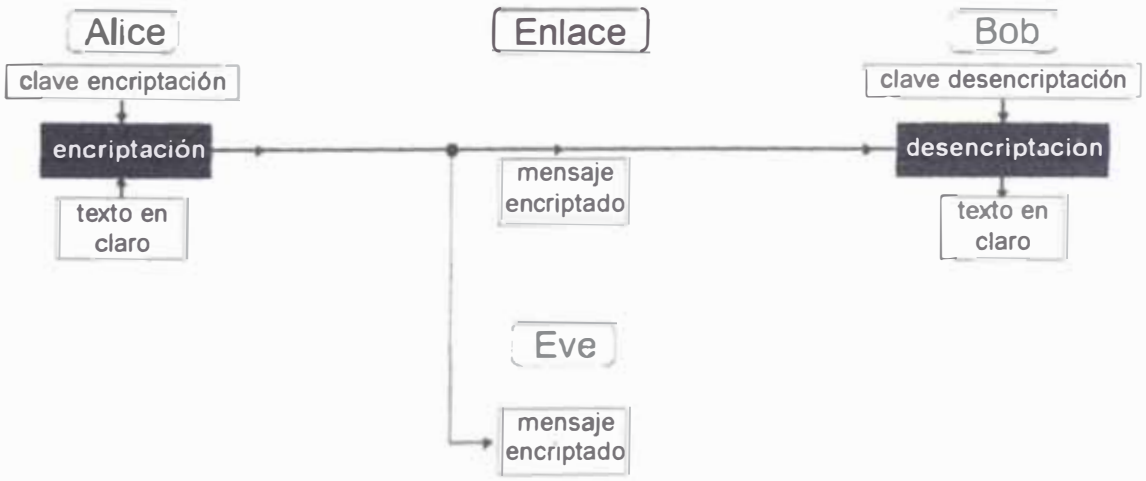


Figura 7: Alice mediante un algoritmo y una clave encripta el texto en claro. Bob realiza lo mismo para desencriptar el mensaje.

Existen dos protocolos de comunicación entre el emisor Alice y el receptor Bob: ***privado*** y ***público***. Y los respectivos algoritmos de criptografía pueden ser ***simétricos*** ó ***asimétricos***.

En el protocolo privado Alice y Bob utilizan claves secretas que sólo ellos conocen, en el protocolo público la clave de encriptación es pública mientras que la clave de desencriptación es secreta.

Los algoritmos simétricos usan la misma clave de encriptación y desencriptación. Los algoritmos asimétricos usan diferentes claves de encriptación y desencriptación.

1.2 Distribución de una Clave Privada

La distribución de una clave privada es un método cuya seguridad depende de la seguridad de intercambiar la clave Alice y Bob. Durante la segunda guerra mundial los alemanes usaron la famosa máquina Enigma, que era una compleja máquina de criptografía que confiaba su seguridad en la distribución de una clave privada que era conocida únicamente al receptor del mensaje. El protocolo más conocido de distribución de una clave privada es el creado por Gilbert Vernan en 1917 que trabajaba en la compañía "American Telephone and Telegraph" y consistía en utilizar una clave aleatoria tan grande como el mensaje a encriptar este método es llamado el ***one-time pad*** (cuaderno de un solo uso) porque las claves se daban en cuadernos, en el cual cada hoja era una clave, que después de utilizar se arrancaba y destruía.

1.2.1 Algoritmo One-Time Pad

El algoritmo One-Time Pad es un algoritmo simétrico y es el único que es absolutamente seguro contra un espía de poder computacional ilimitado, siempre y cuando la clave sea aleatoria, del mismo tamaño del texto en claro y usada una sola vez, esto fue demostrado por Claude Shannon (16).

Dado el alfabeto[23] $A = \{0, 1, \ldots, n-1\}$, un texto en claro $m = m_1 m_2 m_3 \ldots m_L \quad donde \quad m_i \in A$ y una clave de la misma longitud $k = k_1 k_2 k_3 \ldots k_L \quad donde \quad k_i \in A$. El algoritmo de encriptación empleado por Alice

[23] Un alfabeto es un conjunto de símbolos alfanuméricos utilizados para escribir un mensaje.

produce el mensaje encriptado $c = c_1 c_2 c_3 \ldots c_L \quad donde \quad c_i \in A$, utilizando la operación $c_i = m_i \oplus k_i$, $1 \leq i \leq L$ ($\oplus$ denota la adición módulo n)

Al aplicar Bob la misma operación al mensaje encriptado se reconstruye el texto en claro. En la mayoría de las aplicaciones se utiliza $n=2$, por tanto todos los mensajes estarán en binario.

Pero el gran inconveniente de este método y la principal razón de no ser utilizado actualmente es el problema de la distribución segura de la clave. Pues para que la clave este completamente segura es necesario que Alice Y Bob se encuentren personalmente y la intercambien, caso que no siempre es posible Este problema es conocido como el CATCH 22[24] de la criptografía (17) y cuya solución la ofrece la criptografía cuántica.

1.3 Distribución de una Clave Pública

En 1970, James Ellis ideo una nueva forma de comunicación donde la clave de encriptación es pública y por tanto Alice y Bob no necesitan ninguna clave secreta para encriptar. La seguridad de este método se basa en los complejos cálculos matemáticos que debería realizar el espía para descubrir la clave de desencriptación. Es decir que la seguridad aquí solo depende de la potencia de cálculo del espía

1.3.1 Algoritmo RSA

En 1978, Ronalt Rivest, Adi Shamir y Leonar Adleman, desarrollaron el primer algoritmo práctico de distribución de una clave pública conocido como RSA. Es el algoritmo más usado en la actualidad. Es utilizado por compañías de software como Microsoft, Apple, Sun y Novell, a nivel de hardware se utiliza en equipos de seguridad de teléfonos, tarjeta de red Ethernet y smart cards; en Internet se encuentra incorporado en la mayoría de protocolos de seguridad S/MIME, SSL y S/WAN. Es también usado internamente en muchas instituciones, incluyendo oficinas gubernamentales de USA, grandes compañías y universidades (18).

Se trata un algoritmo asimétrico donde la clave de encriptación es pública, básicamente consiste en lo siguiente. Bob genera un número entero producto de dos números primos.

[24] **CATCH 22**: "Antes que Alice y Bob puedan comunicarse en secreto, ellos deben primero poder comunicarse en secreto"

Él publica el número entero, más no los factores primos. Alice usando el algoritmo RSA utiliza este número entero para encriptar su mensaje y enviarlo a Bob. Este mensaje encriptado sólo se puede descifrar usando los números primos. Un espía tendría que factorizar el número entero para obtener los números primos y es allí donde radica la seguridad de este algoritmo. Las computadoras actuales tienen dificultad para factorizar números grandes. Hoy el algoritmo clásico más rápido para factorizar un número entero N es el Number Field Sieve (NFS) (18) que requiere un número de operaciones del orden de $e^{1.9(\ln N)^{1/3}(\ln \ln N)^{2/3}}$ Por ejemplo para factorizar el número de 200 dígitos:

N=27997833911221327870829467638722601621070446786955428537560009929326
128400107609345671052955360856061822351910951365788637105954482006576775098580557613579098734950144178863178946295187237869221823983

Y obtener sus dos factores primos p y q, se tardaría aproximadamente 55 años en una sola computadora de 2.2 GHz AMD Opteron. El 9 de mayo del 2005 (19), F. Bahr, M. Boehm, J. Franke, and T Kleinjung, usando una red de 80 computadoras de 2 2 GHz AMD Opteron consiguieron factorizarla en 3 meses, obteniendo:

p=35324619344027701212726049781984643686711974001976250236493034687761212536794232000585479565280883 49

q=79258699544783330333470858414800596877379758573642199607343303414557678728181521353814093047401854 67

Según el Centro de Computación Cuántica de la Universidad de Oxford (1) una máquina actual tardaría miles de millones de años en factorizar una cifra de mil dígitos.

Ejemplo de encriptación utilizando el algoritmo RSA

1. Bob elige dos números primos bastantes grandes p y q, y obtiene un número entero $N = pq$.
   - Usemos números pequeños para comprender el funcionamiento, sea $p = 3$ y $q = 7$; $N - 21$
2. Luego elige un número c que no tiene común divisor con el producto $(p-1)(q-1)$.

- Como $(3-1)(7-1)=12$, elegimos por ejemplo c 5 que no tiene común divisor con 12

3. Bob calcula un d tal que: $(cd) \bmod (p-1)(q-1)=1$.

   - $(5d) \bmod 12 = 1$ entonces d 5

4. Bob envía por un canal no seguro, por ejemplo Internet o teléfono, los números N y c, pero no p ni q ni d. N y c constituyen la clave pública.

   - N 21; c =5

5. Alice desea enviar un mensaje a Bob el cual puede ser representado por el número N, $a < N$ (Si el número a es N o es demasiado grande se puede dividir en varias partes y enviarlas por separado[25].). Alice calcula el mensaje encriptado:

   $b = a^c \bmod N$

   - Sea a 11 el texto en claro entonces el mensaje encriptado a enviar es $b = 11^5 \bmod 21 = 2$

6. Alice envía el mensaje encriptado b a Bob y él calcula $b^d \bmod N$

   - $a = 2^5 \bmod 21 = 11$

De esa manera Bob recupera el mensaje original

En la Tabla 1 se muestra todos los casos posibles cuando N 21 y c 5 Se observa que en algunos el mensaje encriptado es igual que el texto en claro y además vemos que ningún mensaje encriptado se repite siempre y cuando $a < N$:

a (texto en claro secreto que desea enviar Alice a Bob)	b (mensaje encriptado)	a (mensaje secreto desencriptado por Bob)
0	0	0
1	1	1
2	11	2
3	12	3

[25] Si a fuese igual a N entonces el mensaje encriptado sería igual que para a 0, es decir b 0 (Ya que $b = a^c \bmod N$) lo que causaría una confusión al momento de desencriptar. Y si a es mayor que N entonces su encriptación será igual que el de otro que es menor que N, pues cuando se realiza la operación mod a N el resultado es siempre menor que N, es decir que la cantidad de resultados encriptados es limitada.

4	16	4
5	17	5
6	6	6
7	7	7
8	8	8
9	18	9
10	19	10
11	2	11
12	3	12
13	13	13
14	14	14
15	15	15
16	4	16
17	5	17
18	9	18
19	10	19
20	20	20

Tabla 1: Encriptacion desde 0 hasta 20 utilizando el algoritmo RSA.

1.3.2 Otros algoritmos clásicos

Además del RSA existen otros algoritmos clásicos (20) como DSA[26] (Digital Signature Algorithm o Algoritmo de Firma Digital[27]), AES[28] (Advanced Encryption Standard), el ElGamal[29], ECDSA[30] (Elliptic Curve Digital Signature Algorithm), etc Sin embargo todos estos sistemas tienen algo en común: se basan en las matemáticas. Su seguridad depende de la potencia de cálculo del equipo que posea el espía para poder realizar los complejos cálculos que se necesita para romper la seguridad, por lo que estos algoritmos no son absolutamente seguros.

[26] DSA: Se hizo público el 30 de agosto de 1991, este algoritmo sirve para firmar y no para encriptar información. Una desventaja de este algoritmo es que requiere mucho más tiempo de cómputo que el RSA.

[27] Firma digital: Es un método criptográfico que asocia la identidad de una persona al mensaje. Se obtiene aplicando un algoritmo, denominado función hash, al mensaje para obtener un número que lo identifica unívocamente, luego a este valor "hash" se le aplica el algoritmo de firma digital empleando una clave privada y se adjunta el resultado al mensaje. La persona que reciba el mensaje podrá comprobar la firma usando la clave pública del firmante para obtener el valor hash y luego comprobar que es correcto al aplicar la función hash al mensaje.

[28] AES: Fue anunciado el 26 de noviembre del 2001 y desde el 2006 es el algoritmo más popular en criptografía simétrica. Es usado actualmente a gran escala por el gobierno de los Estados Unidos para encriptar información clasificada (TOP SECRET).

[29] ElGamal: Es un algoritmo de criptografía asimétrica, fue descrito por Taher Elgamal en 1984. Puede ser utilizado tanto para generar firmas digitales como para encriptar y desencriptar.

[30] ECDSA: Es una variación del DSA, emplea operaciones sobre puntos de curvas elípticas. La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que el RSA. Ser usa tanto para firmar o encriptar.

Capítulo 2

Criptografía Cuántica

En la criptografía clásica actual la seguridad de los protocolos depende de la complejidad matemática de los algoritmos utilizados y de la limitada potencia de cálculo de las computadoras actuales, como por ejemplo la factorización de números muy grandes utilizado en el algoritmo clásico RSA. Más aún ya se predice que en unos 20 años (2) las primeras computadoras cuánticas podrán resolver fácilmente los problemas que son inmensamente difíciles o imposibles para las computadoras actuales y por tanto todos los protocolos de seguridad quedarán obsoletos. Cabe mencionar que ya existen dos algoritmos cuánticos que factorizan números. algoritmo de Shor (3) y el algoritmo de las Sumas de Gauss (4).

Por esa razón se debe buscar un algoritmo de encriptación que sea absolutamente seguro tanto para una computadora clasica como para una cuántica. La solución, como demostró Shannon (16) es utilizar el algoritmo One-Time Pad, aunque subsiste el problema del intercambio de claves, pues para que sea absolutamente seguro Alice y Bob tendrían que encontrarse personalmente para intercambiar dicha clave, lo cual no es práctico. Esta es la principal razón por la que no es usado en la actualidad, ya que el intercambio de la clave, estando separados, abre la posibilidad de ser interceptada por algún espía. En 1984 Bennett y Brassard descubrieron como usar las propiedades de la Física Cuántica para obtener una clave y estar al mismo tiempo seguros de no haber sido interceptados Con ello se dio inicio a la Criptografía Cuántica entendida como la criptografía que utiliza principios de la Mecánica Cuántica para crear una clave secreta simétrica.

2.1 Vulnerabilidad de algoritmos clásicos: Algoritmo de Shor

Richard J. Hughes (21), asumiendo correcta la ley de Moore donde la velocidad de los procesadores se duplica aproximadamente cada 18 meses, realiza una proyección interesante para el año 2042, donde 100 computadoras clásicas de esa época tardarían 2×10^{22} años en factorizar un número de 1234 dígitos (4096 bits), en cambio si se tuviera una computadora cuántica de tan sólo 100 MHz tardaríamos 4.8 horas.

Otro informe es del Centro de Computación Cuántica de la Universidad de Oxford (1) donde estima que una máquina actual tardaría miles de millones de años en factorizar una cifra de mil dígitos mientras que una computadora cuántica lo lograría en tan solo 20 minutos. El problema es que todavía no existe un computadora cuántica lo suficientemente desarrollada para lograrlo[31].

Pero las investigaciones hacen suponer que dentro de 20 años ya tendremos computadoras cuánticos operativas (2) y entonces todos los sistemas basado en el RSA serán obsoletos y todas las claves vulnerables

El Algoritmo de Shor (3) es un algoritmo de factorización que combina los principios de la mecánica cuántica y la teoría de números.

Como se menciono anteriormente factorizar en una computadora clásica un número entero N requiere en el mejor de los casos (18) una cantidad de operaciones que crece exponencialmente con N y es del orden de $e^{1.9(\ln N)^{1/3}(\ln \ln N)^{2/3}}$. En cambio se estima que el algoritmo de factorización de Shor en una computadora cuántica (22) requeriría un número de operaciones que crece polinomialmente con N y es del orden de $(\ln N)^2 (\ln \ln N)(\ln \ln \ln N)$.

En la Figura 8 se muestra que para un número N de 4 dígitos, el algoritmo clásico requiere 879 operaciones en cambio el algoritmo cuántico de Shor solamente 150. A

[31] En setiembre del 2009 físicos de la Universidad de Bristol, Inglaterra, ejecutan el algoritmo de Shor en un chip de silicio que en lugar de usar electricidad utiliza cuatro fotones (4 qubits) que viajan a través de guías por el chip factorizando el número 15 (61). La primera vez que se probo el algoritmo de Shor fue en el 2001 por IBM y la Universidad de Stanford, el número que se factorizó fue el 15 pero usando una computadora cuántica de 7 qubits y técnicas de Resonancia Magnética Nuclear (57).

medida que el número N aumenta la diferencia se incrementa aún más. Por ejemplo (Figura 9) para un número N de 300 dígitos, el algoritmo clásico requiere 3.1902×10^{25} operaciones en cambio el algoritmo cuántico de Shor solamente 5.8575×10^{6}.

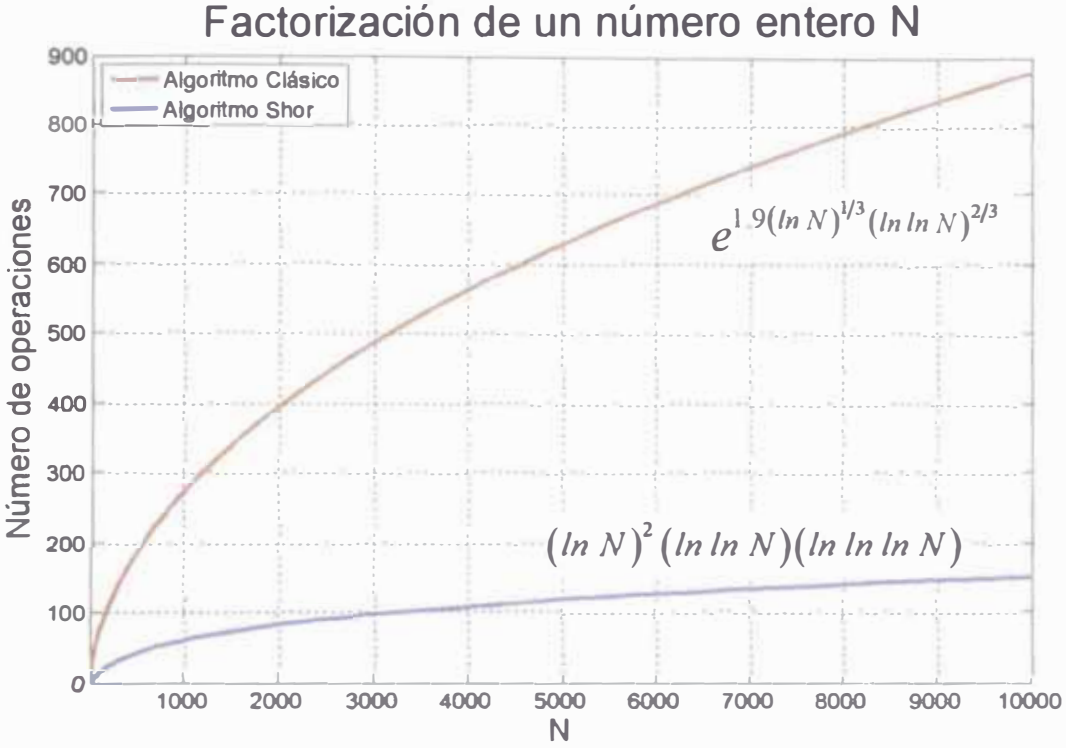


Figura 8: Gráfica para números N de 0 a 4 dígitos ($0 \leq N < 10^4$)

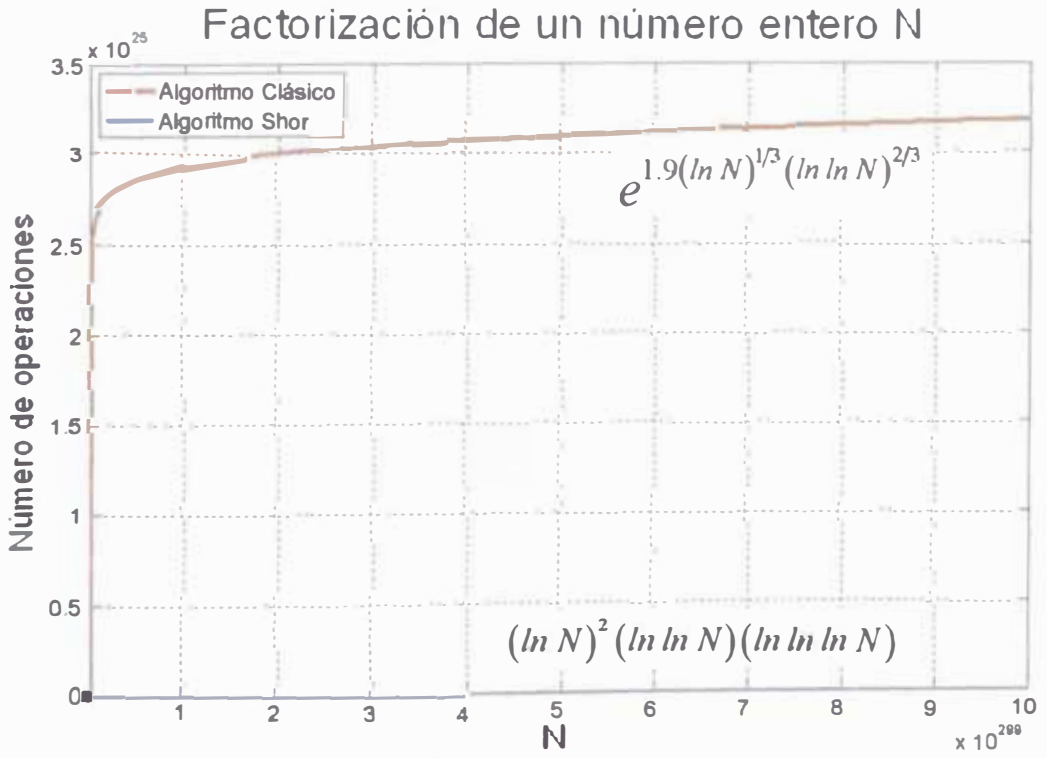


Figura 9: Gráfica para números N de 0 a 300 dígitos ($0 \leq N < 10^{300}$)

El algoritmo de Shor depende de la siguiente propiedad en la teoría de números: "La función $f(x) = a^x \bmod N$ es periódica cuando a es un entero coprimo[32] de N" (23). Si N es el número entero que se quiere factorizar, el objetivo es hallar el menor periodo r par de $f(x)$

Como $f(0) = a^0 \bmod N = 1$ entonces se cumple que $f(r) = a^r \bmod N = 1$, $f(2r) = a^{2r} \bmod N = 1$, $f(3r) = a^{3r} \bmod N = 1$ y así sucesivamente.

Cuando r es par[33]:

$$\left(a^{r/2}\right)^2 \bmod N = 1$$

$$\left[\left(a^{r/2}\right)^2 - 1\right] \bmod N = 0$$

$$\left[\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)\right] \bmod N = 0$$

Como se observa, el producto $\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right)$ es un entero múltiplo de N, en el algoritmo RSA el número N es producto de dos primos p y q entonces $\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) = c_p c_q (pq)$, donde c_p y c_q son números naturales, luego $\left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) = (c_p p)(c_q q)$ por tanto $\left(a^{r/2} - 1\right) = c_p p$ y $\left(a^{r/2} + 1\right) = c_q q$ y finalmente $mcd\left(a^{r/2} - 1, N\right)$ y $mcd\left(a^{r/2} + 1, N\right)$ son los factores primos de N:

$mcd\left(a^{r/2} - 1, N\right) = mcd\left(c_p p, pq\right) = p$ Primer factor primo[34]

$mcd\left(a^{r/2} + 1, N\right) = mcd\left(c_q q, pq\right) = q$ Segundo factor primo

Clásicamente realizar el cálculo para hallar r requiere probar con todos los x hasta observar la presencia del periodo. En cambio el algoritmo de Shor utiliza la superposición cuántica y realiza una computación paralela para poder evaluar todos los

[32] Dos números son coprimos si su máximo común divisor es 1

[33] Si r es impar entonces $a^{r/2}$ no es entero. Entonces elegimos como periodo a $2r$.

[34] Si c_p es múltiplo de q entonces el mcd es pq y se tendrá que intentar con otro r o a.

valores de x al mismo tiempo. En la Figura 10 se muestra el modelo del circuito cuántico para efectuar este cálculo[35].

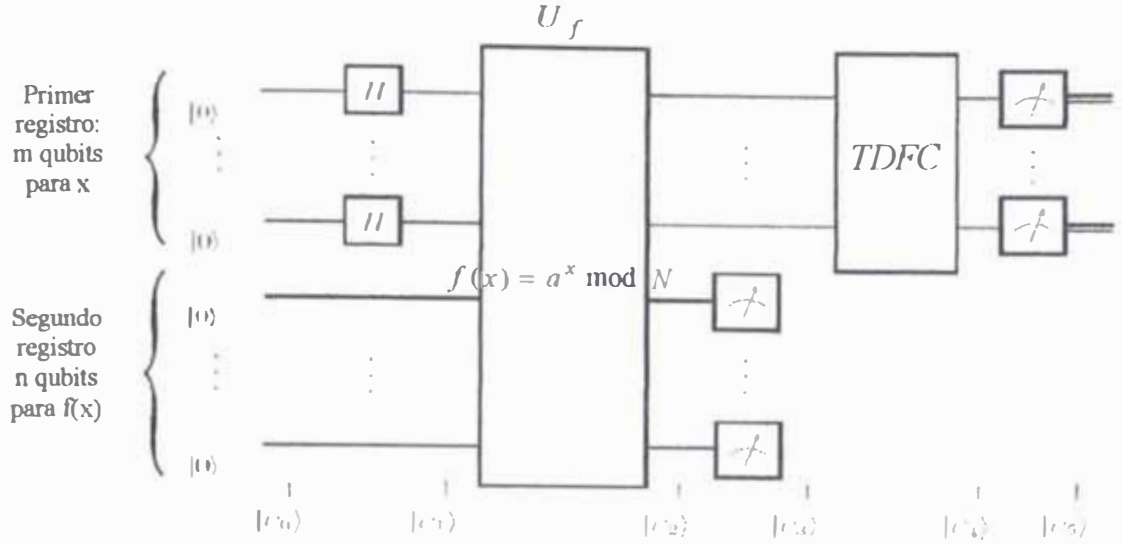


Figura 10: Circuito cuántico para hallar el periodo r de $a^x \bmod N$.

Ejemplo de factorización del número $N = 21$ usando el algoritmo de Shor

1. Se elige un número aleatorio coprimo de N, por ejemplo $a = 2$.

2. Cálculo de n: Debe ser lo suficientemente grande para almacenar el máximo valor de $f(x) = a^x \bmod N$. Como el resto de una división no puede ser mayor o igual que el número N entonces se elige[36] $n > \log_2 N = \log_2 21 = 4.39$, por tanto $n=5$.

3. Cálculo de m: Debe ser lo suficientemente grande para que contenga varios periodos. Como $f(r) = a^r \bmod N = 1$, entonces el máximo r ocurre cuando $a = 2$, luego $2^r \bmod N = 1$, es decir que $2^r = cN + 1$, donde c es un número natural, como $2^r > r$ entonces $cN + 1 > r$ ó $cN \geq r$. Para estar seguros de observar como mínimo 2 periodos podemos tener valores de x hasta $2cN$.

[35] El circuito cuántico para realizar $f(x) = a^x \bmod N$ requiere de una configuración extensa de muchas compuertas cuánticas, en (59) se muestra el circuito completo.

[36] Tengamos en cuenta que n qubits puede representar números desde 0 hasta 2^n-1. Como el resto debe ser menor que N, entonces se elige un n lo suficientemente grande 2^n-1=N, es decir 2^n>N.

Pero para obtener una mejor la distribución estadística se acostumbra usar un valor mucho mayor, entre N^2 y $2N^2$. En este ejemplo se toma N^2, entonces $m > \log_2 N^2 = 2\log_2 N = 8.78$, por tanto $m = 9$.

4. Se prepara un primer registro con $m = 9$ qubits para representar los valores de x inicializados en el estado $|0\rangle$ cada uno. Y un segundo registro con n 5 qubits también cada uno inicializados en $|0\rangle$ para representar los valores de $f(x) = a^x \bmod N$ Ambos forman el estado inicial $|\psi_0\rangle = |000000000\rangle|00000\rangle = |0\rangle|0\rangle$

5. A los m qubits del primer registro se le aplica el operador Hadamard (Apéndice A) para preparar una superposición uniforme de estados.

$$|\psi_1\rangle = H^{\otimes 9}|0\rangle|0\rangle = \frac{1}{\sqrt{512}}\sum_{x=0}^{511}|x\rangle|0\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{512}}(|0\rangle + |1\rangle + |2\rangle + \cdots + |511\rangle)|0\rangle$$

6. La compuerta U_f calcula la función $f(x) = 2^x \bmod N$ para la superposición de los m qubits y almacena el resultado en los n qubits del segundo registro Como $f(x)$ es periódica se espera que el segundo registro muestre valores que se repitan periódicamente al recorrer x.

7. Se reordena el resultado para notar mejor como sólo algunos estados del segundo registro son posibles, se puede ver las cantidad de veces que se repite un valor del segundo registro·

$$|\psi_2\rangle = \frac{1}{\sqrt{512}}[(|0\rangle + |6\rangle + |12\rangle + \ldots + |504\rangle + |510\rangle)|1\rangle +$$
$$(|1\rangle + |7\rangle + |13\rangle + \ldots + |505\rangle + |511\rangle)|2\rangle +$$
$$(|2\rangle + |8\rangle + |14\rangle + \ldots + |506\rangle)|4\rangle +$$
$$(|3\rangle + |9\rangle + |15\rangle + \ldots + |507\rangle)|8\rangle +$$
$$(|4\rangle + |10\rangle + |16\rangle + \ldots + |508\rangle)|16\rangle +$$
$$(|5\rangle + |11\rangle + |17\rangle + \ldots + |509\rangle)|11\rangle]$$

En cada superposición del primer registro se observa el periodo de la función en este ejemplo 6, en este punto este periodo es aún desconocido. Entonces para descubrirlo sólo basta analizar la superposición del primer registro para cualquier estado del segundo registro.

8. Se realiza una medición cuántica del segundo registro la cual hará que colapse en uno de sus estados posibles $f(x)=\{1,2,4,8,11,16\}$. Por ejemplo si colapsa en $|8\rangle$, se obtiene:

$$|\psi_3\rangle = \frac{1}{\sqrt{85}}(|3\rangle+|9\rangle+|15\rangle+\ldots+|507\rangle)|8\rangle = \frac{1}{\sqrt{85}}\sum_{a=0}^{84}|6a+3\rangle|8\rangle$$

9. Sin embargo el periodo no se hará evidente ante una medición directa del primer registro pues el sistema colapsaría en uno de los estados $|x\rangle$ y todos tienen la misma probabilidad de 1/85=0.0118, y se perdería toda la información acerca del periodo. En la Figura 11 mostramos la distribución de probabilidades.

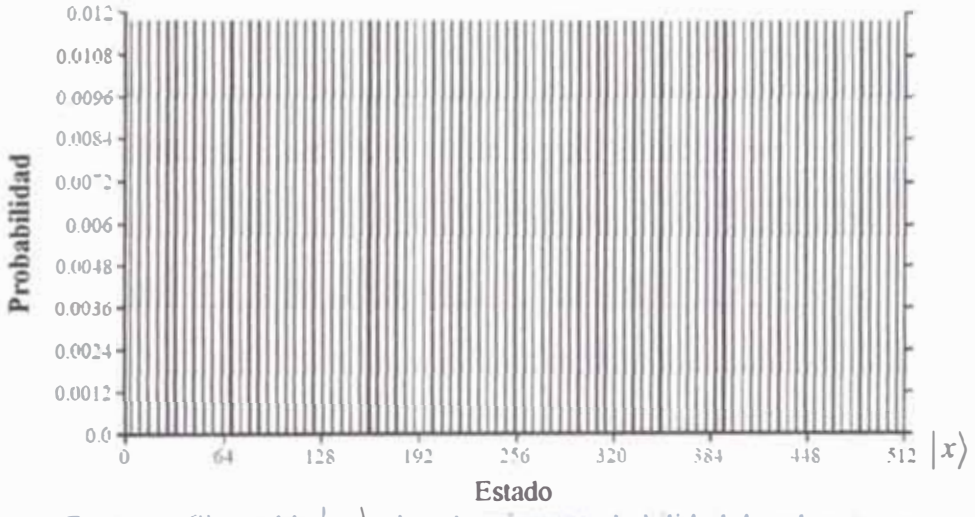


Figura 11: Si se mide $|\psi_3\rangle$, tiene la misma probabilidad de colapsar en cualquiera de los 512 estados.

10. Como el periodo no es posible observarlo en el "dominio temporal"[37], en este caso dominio de estados del primer registro, se utiliza la Transformada Discreta de Fourier Cuántica (Apéndice A) para pasar a un "dominio frecuencial". La Transformada Discreta de Fourier Cuántica transforma una función periódica r en una nueva función periódica con periodo proporcional a $1/r$.

El uso de los términos "dominio temporal" y "dominio frecuencial" proviene a que inicialmente la transformada de Fourier se usaba en el estudio de señales dependientes del tiempo.

$$|k\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i jk/N} |j\rangle$$

Cuando la TDFC se aplica a cada estado para pasar al dominio de frecuencias:

$$|\psi_4\rangle = TDFC(|\psi_3\rangle)$$

$$= TDFC\left(\frac{1}{\sqrt{85}} (|3\rangle + |9\rangle + |15\rangle + \ldots + |507\rangle) \right) |8\rangle$$

$$= \frac{1}{\sqrt{85}} \left(\begin{array}{l} \frac{1}{\sqrt{512}} \sum_{j=0}^{511} e^{2\pi i j3/512} |j\rangle + \frac{1}{\sqrt{512}} \sum_{j=0}^{511} e^{2\pi i j9/512} |j\rangle + \frac{1}{\sqrt{512}} \sum_{j=0}^{511} e^{2\pi i j15/512} |j\rangle + \\ \ldots + \frac{1}{\sqrt{512}} \sum_{j=0}^{511} e^{2\pi i j507/512} |j\rangle \end{array} \right) |8\rangle$$

$$= \frac{1}{\sqrt{512}} \frac{1}{\sqrt{85}} \left(\sum_{j=0}^{511} \left(e^{2\pi i j3/512} + e^{2\pi i j9/512} + e^{2\pi i j15/512} + \ldots + e^{2\pi i j507/512} \right) |j\rangle \right) |8\rangle$$

$$= \frac{1}{\sqrt{512}} \frac{1}{\sqrt{85}} \left(\sum_{j=0}^{511} \left(\sum_{a=0}^{84} e^{2\pi i \frac{j(6a+3)}{512}} \right) |j\rangle \right) |8\rangle$$

11. Ahora se mide el primer registro el cual hará que colapse a un estado múltiplo de *1/r*. El sistema colapsa en un estado $|j\rangle$ con una probabilidad:

$$p = \frac{1}{512 \times 85} \left| \sum_{a=0}^{84} e^{2\pi i \frac{j(6a+3)}{512}} \right|^2 = \frac{1}{512 \times 85} \left| e^{2\pi i \frac{j(3)}{512}} \sum_{a=0}^{84} \left(e^{2\pi i \frac{j(6a)}{512}} \right) \right|^2$$

$$= \frac{1}{512 \times 85} \left| \sum_{a=0}^{84} \left(e^{2\pi i \frac{j(6a)}{512}} \right) \right|^2 = \frac{1}{512 \times 85} \left| 1 + \sum_{a=1}^{84} \left(e^{2\pi i \frac{j(6a)}{512}} \right) \right|^2$$

Cuando $6j$ es múltiplo de 512. La probabilidad es máxima $p = \frac{1}{512 \times 85} |1 + 84|^2 = 0.166$. En este caso *6j=512k*, donde *k* es natural, entonces $\frac{j}{512} = \frac{k}{6}$ es múltiplo de la frecuencia buscada 1/6 hasta ahora desconocida.

Además para valores de j tal que $6j$ es aproximadamente múltiplo de 512 también se cumplirá que $j/512$ es aproximadamente múltiplo de $1/6$ y por tanto se podrá deducir la frecuencia usando el método de las fracciones continuas[38].

Graficando las probabilidades[39] se obtienen máximos en: En j = 0 (p=16.6%), 85 (p=11.39%), 171 (p=11.39%), 256 (p=16.6%), 341 (p=11.39%) y 427 (p=11.39%). (Figura 12).

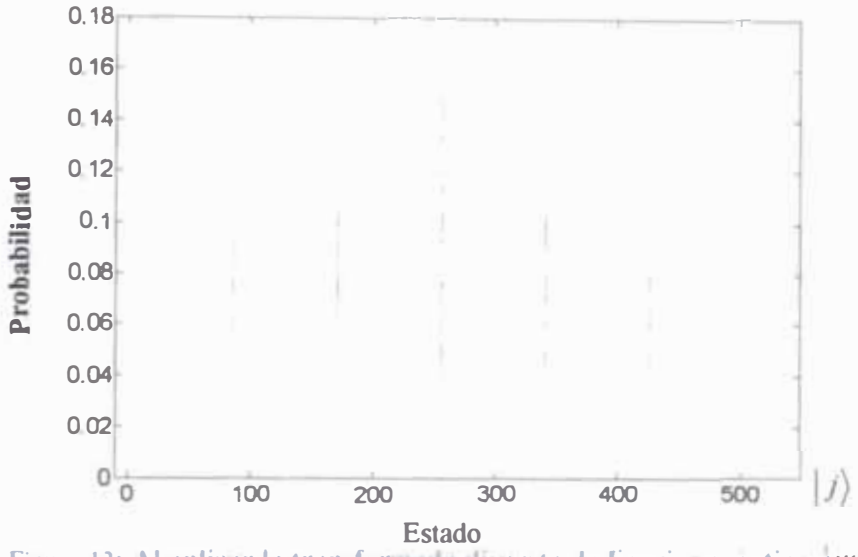


Figura 12: Al aplicar la transformada discreta de Fourier cuántica, $|\psi_4\rangle$ tiene más probabilidad de colapsar en algunos estados.

12. Si al medir el primer registro el sistema colapsa por ejemplo en $|85\rangle$:

$$|\psi_5\rangle = \frac{1}{\sqrt{512}}\frac{1}{\sqrt{85}}\left(\sum_{j=0}^{511}\left(\sum_{a=0}^{84} e^{2\pi i\frac{j(6a+3)}{512}}\right)|j\rangle\right)|8\rangle$$

$$= \frac{1}{\sqrt{512}}\frac{1}{\sqrt{85}}\left(\sum_{a=0}^{84} e^{2\pi i\frac{85(6a+3)}{512}}|85\rangle\right)|8\rangle$$

Entonces la fracción 85/512 es múltiplo aproximado de la frecuencia $1/r$.

---

[38] Este método consiste en expandir una fracción de la forma p/q de la siguiente forma, donde a_0 es no negativo y $a_{1,2,\ldots n}$ enteros positivos:

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

[39] Analíticamente también se puede hallar estos máximos a partir la fórmula de la serie geométrica $\sum_{k=1}^{n} e^{ikx} = \frac{e^{ix}\left(1-e^{inx}\right)}{1-e^{ix}}$ y aplicando criterios para hallar los valores extremos de la función lo que conduciría a una ecuación transcendental que se resolvería usando métodos numéricos.

Aquí culmina el aporte de la computación cuántica, lo siguiente es aplicar aritmética clásica para hallar el periodo r.

13. Se aplica el método de expansión a fracciones continuas para obtener fracciones que converjan a $\frac{85}{512}$.

$$\frac{85}{512} = 0 + \frac{1}{6 + \frac{2}{85}} = 0 + \frac{1}{6 + \frac{1}{42 + \frac{1}{2}}}$$

Por tanto las fracciones que convergen a $\frac{85}{512}$ son $\frac{1}{6}$, $\frac{42}{253}$ y $\frac{85}{512}$. Y todas son múltiplos aproximados de $1/r$.

14. Es decir que 1/r puede ser 1/6, 1/253, 1/512, Pero como r no puede ser mayor que N entonces elegimos aquella fracción cuyo denominador no exceda a $N=21$, es decir 1/6. Por tanto el periodo de $f(x)$ es $r = 6$.

15. Verificamos[40] que. $2^6 \bmod 21 = 1$

Entonces $(2^6\text{-}1) \bmod 21=0$

$[(2^3+1)(2^3\text{-}1)] \bmod 21=0$

Esto significa que 21 divide a $[(2^3+1)(2^3\text{-}1)]$

16. Hallamos el mcd[41] y así obtenemos los factores que dividen a $N=21$, estos serán los factores primos:

$mcd(2^3+1,21) = 3$

$mcd(2^3\text{-}1,21) = 7$

17. Entonces hemos logrado factorizar $N = 21 = 3 \times 7$

Otro ejemplo de factorización usando el algoritmo de Shor se puede encontrar en la tesis doctoral de Anthony Hams (24) donde factoriza el número 15.

[40] Si r es impar elegimos 2r.
[41] Para hallar el mcd usamos el algoritmo de Euclides.

Observación:

En el paso 12 se asume que el sistema colapsa en el estado $|85\rangle$, pero también existe la probabilidad que colapse en otros estados, analicemos si obtenemos los factores primos en estos estados.

- Estado $|0\rangle$: Anula la información acerca de r. No sirve y debemos iniciar nuevamente todo el proceso.
- Estado $|85\rangle$: Si funciona (ya se verificó).
- Estado $|171\rangle$: $\frac{171}{512} = 0 + \frac{1}{2 + \frac{170}{171}} = 0 + \frac{1}{2 + \frac{1}{1 + \frac{1}{170}}}$

  Las fracciones que convergen a $\frac{171}{512}$ son $\frac{1}{2}$, $\frac{1}{3}$ y $\frac{171}{512}$. La fracción con denominador más pequeño es $\frac{1}{2}$ entonces $r=2$. Pero $2^2 \bmod 21 = 4$, no cumple pues debería ser 1. Entonces $r=2$ no sirve.

  La fracción siguiente es $\frac{1}{3}$ no cumple pues $r = 3$ es impar, entonces elegimos el doble es decir $r = 6$ que si cumple.
- Estado $|256\rangle$: $\frac{256}{512} = 0 + \frac{1}{2}$

  Las fracciones que convergen a $\frac{256}{512}$ son $\frac{1}{2}$ y $\frac{256}{512}$. La fracción más cercana es $\frac{1}{2}$ entonces $r=2$ pero como se demostró este valor no cumple.
- Estado $|341\rangle$: $\frac{341}{512} = 0 + \frac{1}{1 + \frac{171}{341}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{170}{171}}} = 0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{170}}}}$

  Las fracciones que convergen a $\frac{341}{512}$ son $\frac{1}{1}$, $\frac{1}{2}$, $\frac{2}{3}$ y $\frac{341}{512}$. La fracción $\frac{2}{3}$ no cumple pues r no puede ser impar entonces elegimos $r = 6$ que si cumple.
- Estado $|427\rangle$: $\frac{427}{512} = 0 + \frac{1}{1 + \frac{85}{427}} = 0 + \frac{1}{1 + \frac{1}{5 + \frac{2}{85}}} = 0 + \frac{1}{1 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}}}$

Las fracciones que convergen a $\frac{427}{512}$ son $\frac{1}{1}, \frac{5}{6}, \frac{211}{253}$ y $\frac{427}{512}$. La fracción $\frac{5}{6}$ es la más cercana entonces $r = 6$. Como ya se verificó este valor si factoriza N.

De las seis posibilidades sólo dos estados logran dar descubrir un r que logra factorizar N: El estado $|85\rangle$ (11.39%) y es estado $|427\rangle$ (11.39%), por tanto la probabilidad de tener éxito seguro en este ejemplo es 22.78%. Y de forma indirecta los estados $|171\rangle$ (11.39%) y $|341\rangle$ (11.39%) que dan un 22 78%. En total la probabilidad de encontrar los números primos es 45.56%.

Este ejemplo muestra como el algoritmo cuántico de Shor en combinación con algoritmos clásicos logra factorizar números enteros y cuando las computadoras cuánticas sean una realidad, todos los protocolos basados en RSA serán vulnerables y por tanto será necesario ir a un método de encriptación más seguro incluso para las computadoras cuánticas. Estos protocolos ya existen y uno de ellos es el BB84, protocolo que se ha realizado con éxito en esta tesis.

2.2 Seguridad de la Criptografía Cuántica

La Criptografía Cuántica genera claves inviolables por 3 razones vinculadas al principio de la mecánica cuántica.

1. El principio de incertidumbre de Heisenberg que afirma que existen pares de propiedades que son incompatibles en el sentido que la medida de una de ellas vuelve aleatoria el valor de la otra, estas propiedades en criptografía cuántica son las polarizaciones de los fotones de bases conjugadas.

2. Al medir un estado cuántico este colapsa indefectiblemente en otro estado (Tercer postulado de la mecánica cuántica) Esto significa que si Eve mide el fotón antes de llegar a Bob lo va a modificar[30] y así a Bob le llegará un fotón en un estado distinto del que envió Alice.

3. Los estados cuánticos no se pueden copiar (Teorema de la no clonación) (25) (26). Esto significa que el espía Eve no puede obtener una copia para analizarla independientemente.

   Demostración: Supongamos que existe un operador que puede copiar un estado en otro $U|\varphi\rangle|\psi\rangle = |\varphi\rangle|\varphi\rangle$, ahora apliquemos el operador a cada estado $|a\rangle$ y $|b\rangle$ por separado, $U|a\rangle|c\rangle = |a\rangle|a\rangle$ y $U|b\rangle|c\rangle = |b\rangle|b\rangle$. Ahora realicemos el producto interno de estas dos $\langle c|\langle a|U^{\dagger}U|b\rangle|c\rangle = \langle a|\langle a||b\rangle|b\rangle$ y obtenemos $\langle a|b\rangle = \langle a|b\rangle^2$ y esto solo se cumple cuando $|a\rangle$ y $|b\rangle$ son ortogonales o son el mismo. Por tanto solo se puede clonar estados a sí mismos o que son ortogonales uno respecto a otro, pero como el espía desconoce el estado original entonces tampoco sabe cuál es el estado ortogonal y no podrá clonarlo.

Esta seguridad se basa en las leyes de la física cuántica, leyes de la naturaleza que son imposibles de violar.

[30] Excepto si Eve tiene la suerte de medir la polarización del fotón en la misma base que fue enviada por Alice, es decir que tiene un 50% de acertar.

2.3 Protocolos de Criptografía Cuántica

Son protocolos que utilizan algoritmos simétricos, específicamente el algoritmo One-Time Pad. Básicamente se tiene cuatro protocolos, dos de ellos utilizan fotones en bases ortogonales (BB84 y B92) y los otros dos fotones entrelazados (E91 y BBM92). En esta tesis desarrollamos el protocolo BB84.

Para realizar la criptografía cuántica se utiliza dos bases conjugadas (Figura 13), cada una con dos polarizaciones ortogonales. La base rectilínea $+ = (|\updownarrow\rangle, |\leftrightarrow\rangle) = \left(\begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\right) = (|0\rangle, |1\rangle) = (|V\rangle, |H\rangle)$ y la base diagonal $\times = (|\nearrow\rangle, |\nwarrow\rangle) = \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}\right) = (|+\rangle, |-\rangle) = (|+45\rangle, |-45\rangle)$.

En cada base la primera polarización representa el bit cero y la segunda polarización el bit uno, esto es arbitrario.

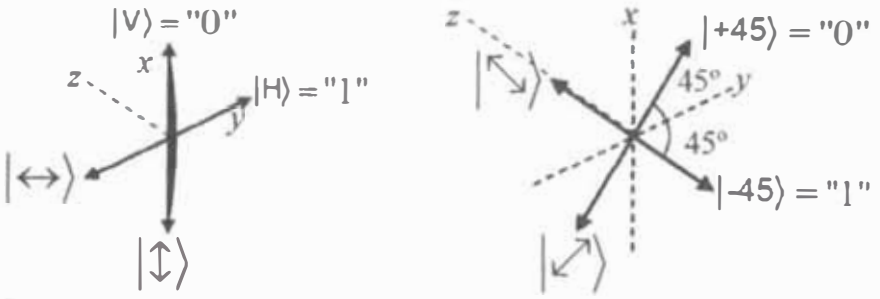


Figura 13: Polarizaciones usadas en el protocolo BB84.

La relación entre estas polarizaciones

El operador Hadamard (apéndice A) definido por $H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$ transforma la base rectilínea $(|0\rangle, |1\rangle)$ a la base ortogonal $(|+\rangle, |-\rangle)$ y viceversa:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$$

También:

$$H|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = |0\rangle$$

$$H|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = |1\rangle$$

Aunque existen diversos protocolos que son variaciones de los comentados en esta tesis, todos son completamente seguros y se puede usar cualquiera, esto evidencia porque muchos de los proyectos de investigación prefieren usar el BB84 (estados ortogonales) y el E91(estados entrelazados) quizás por razones históricas y didácticas. Algunos protocolos cuánticos menos conocidos son SARG04, Six-States, Lo-Chau, CSS, COW, DPS, S09, etc. A continuación se describe detalladamente el protocolo BB84. Los protocolos B92, E91 y BBM92 se describen en el Apéndice B.

2.3.1 Protocolo Cuántico BB84

El protocolo cuántico BB84 (9) utiliza dos bases conjugadas para enviar fotones desde el emisor al receptor mediante un canal cuántico[43]. Como la única manera de determinar exactamente su polarización es conocer en qué base se envió el fotón, al final de la transmisión Alice y Bob deben darse a conocer sus bases, mediante un canal clásico[44], y utilizar aquellas medidas en las que ambos coincidieron en la elección de bases. Por otro lado, en la situación real muchas de las medidas no detectan fotones debido a la atenuación del laser[45] o a que en ese momento no se generó un par en una conversión paramétrica espontanea descendente[46] o porque se perdió en el trayecto o el detector no lo detecto o la presencia de un espia, etc. Por esa razón se envía la suficiente cantidad de fotones para generar una clave en bruto lo suficientemente grande para efectuar las correcciones necesarias y obtener la clave final.

El protocolo cuántico obliga a Bob a informar a Alice, mediante un canal clásico, las posiciones en la secuencia temporal de los fotones que no detecto, para tomar en cuenta sólo los bits detectados. En esta tesis debido a que la distancia entre Alice y Bob en la máquina de criptografía construida es pequeña y porque en cada disparo se envía millones de fotones siempre se cumple que $n_{FotonesEnviados} = n_{FotonesDetectados}$.

[43] El canal cuántico es la línea (aire, fibra óptica o vacío) por donde viajan los fotones desde el emisor Alice al receptor Bob.

[44] El canal clásico es un medio convencional de comunicación que no necesariamente debe estar protegido contra ataques de espías, puede ser una línea telefónica, una señal de radio, una red, internet, etc.

[45] Cuando se usa láseres atenuados usualmente el 90% de medidas no tiene fotones (63).

[46] En una Conversión Paramétrica Espontanea Descendente se tiene una eficiencia entre 10^{-10} y 10^{-12} para un laser incidente de longitud de onda de 450nm (58) y una eficiencia de 10^{-9} para una longitud de onda de 845 nm (62).

Ahora, si un espía intercepta el fotón y mide su polarización, existe la probabilidad que la modifique y que continúe hacia Bob con polarización distinta a la que envió Alice, obteniendo así una clave diferente. Alice y Bob pueden darse cuenta de esta anomalía mediante un procedimiento incluido en el protocolo BB84. El protocolo requiere que antes de enviar el mensaje ambos sacrifiquen de manera aleatoria entre 10% y 50% de sus claves en bruto, esto significa comunicarse los valores de estos bits a través de un canal clásico. Esto permite calcular la Tasa de Error de Qubits (QBER[47]) según la siguiente expresión:

$$QBER = \frac{n_{BitsIguales}}{n_{BitsComparados}} \times 100\%$$

En el artículo de Peter Shor y John Preskill publicado en el 2000 (27) y actualizado en el 2008, muestran que cuando no hay ataque de espías se puede esperar un QBER<11%. Así en el experimento de envío por aire a 144 Km (11) entre las islas La Palma y Tenerife se obtuvo QBER menores de 7% Mediante un procedimiento de corrección de errores, que se describe a continuación, se puede eliminar los bits erróneos y obtener una clave con un QBER de 0%. En la práctica el QBER límite aceptable se adopta de manera práctica, segun condiciones experimentales.

Reconciliación de información (Corrección de errores)

Existen varios métodos que permiten la corrección de errores provenientes del ruido en la línea de transmisión y de una eventual intrusión. En esta tesis usamos una modificación del método de la Cascada (28) donde se usan bloques de tamaño fijo de 4 bits.

1. Alice y Bob permutan aleatoriamente los bits de sus claves, utilizando el mismo generador seudo aleatorio con la misma semilla para que los bits correspondientes a cada uno siempre permanezcan en posiciones iguales pero distintas de la posición original. Esto permite que los posibles errores se distribuyan "uniformemente".

2. Cada uno divide su clave en bloques de 4 bits y calculan la paridad de cada bloque (realizando una operación *XOR* con los 4 bits).

3. Si las paridades son distintas, significa que los bloques de Alice y Bob son distintos entonces se elimina el bloque completo.

[47] Quantum Bit Error Rate.

4. Si las paridades son iguales, significa que los bloques de Alice y Bob son iguales o que ocurrieron pares de errores. El bloque no se elimina pero se elimina el último bit, quedando bloques de 3 bits que permanecen en la clave.

5. Se repiten los pasos 1 al 4 hasta que ya no se encuentren paridades distintas.

Inmediatamente después se realiza la amplificación de privacidad y se calcula nuevamente el QBER para ver si todavía las claves son distintas.

Amplificación de privacidad

La amplificación de privacidad tiene como objetivo reducir la información que tiene Eve; es decir si Eve conoce algunos bits de la clave, luego de la amplificación de privacidad ella conocerá menos bits.

La amplificación de privacidad consiste básicamente en tomar aleatoriamente varios bits de la clave y realizar alguna operación con ellos y el resultado reemplaza a otro bit elegido también aleatoriamente, esto da una gran probabilidad de que Eve mezcle sus bits correctos con los incorrectos, obteniendo un resultado incorrecto que quizás reemplace a un bit correcto.

En esta tesis usamos un método que utiliza el operador XOR (29):

1. De manera aleatoria Alice y Bob seleccionan 2 bits de sus claves, realizan una operación XOR con ellos

2. Elijen otra posición aleatoria de su clave y reemplazan el bit de esa posición por el resultado obtenido en el paso 1.

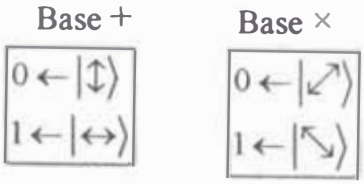
3. Repiten los pasos 1 y 2 una cantidad suficiente de veces, para estar seguro que casi todos los bits se han combinado, por ejemplo una cantidad igual a la cantidad de bits de la clave.

4. El protocolo recomienda que una vez terminada la amplificación hallar nuevamente el QBER, sacrificando otra vez la mitad de la clave obtenida.

5. Si el QBER es cero podemos realizar la transmisión con seguridad, incluso se puede aceptar QBER pequeños, por ejemplo menores de 1%, esto depende de la urgencia, importancia o tipo de mensaje que se desea comunicar.

2.3.1.1 Descripción del protocolo cuántico BB84

1. El mensaje secreto que Alice quiere enviar a Bob tiene ***n*** bits. Para representar estos bits clásicos ambos utilizan la siguiente convención:



2. Alice genera una cadena aleatoria ***a*** de $4n+\delta$ bits[48], luego genera aleatoriamente otra cadena ***b*** con la bases + o × que asignará a cada bit de la cadena ***a***. Por último genera una cadena ***c*** que contiene las polarizaciones de acuerdo a la base y al bit que Alice desea enviar, en el siguiente ejemplo[49] la cantidad de bits enviados por Alice es 48.

3. Alice envía los bits (fotones polarizados) a Bob mediante un canal cuántico. Durante el envío de fotones puede ocurrir que algunos fotones cambien su polarización debido al ruido o presencia de espía. En el ejemplo las celdas amarillas muestran estos cambios de polarización durante el envío.

4. Bob recibe los $4n+\delta$ fotones y mide la polarización de cada uno de ellos utilizando una cadena aleatoria ***b'*** de bases + o ×. Esta medida resulta en polarizaciones que se almacenan en la cadena ***c'*** y por último traduce el resultado en una cadena de bits ***a'***. En el ejemplo, el signo de ? denota el caso cuando no se sabe de antemano en que polarización colapsará el fotón.

---

[48] La clave en bruto que genera el protocolo tiene aproximadamente el 50% de los bits enviados. Y en general se utiliza el 50% para calcular el QBER, de esta forma sólo queda aproximadamente el 25% de los bits enviados. Es decir $\frac{1}{2}\left[\frac{1}{2}(4n+\delta)\right]=n+\frac{\delta}{4}$. Vemos que se tiene un poco más de los ***n*** bits que se necesitan para enviar el mensaje. Este excedente $\frac{\delta}{4}$ se usará para la corrección de errores. El valor δ se determina de manera experimental.

[49] La explicación con detalle del ejemplo se muestra en el párrafo 5.1, aquí se presenta sólo para tener una clara la descripción del protocolo BB84.

5. Alice y Bob utilizando un canal clásico comparan las cadenas ***b*** y ***b'***, descartan las posiciones en la que las bases elegidas difieren y obtiene una subcadena de ***a'*** de longitud aproximada **$(4n+\delta)/2$**, esta cadena se conoce como la clave en bruto (raw key) o clave sin procesar. En el ejemplo las bases iguales están sombreadas de verde, obtienen una clave de 25 bits.

Se observa que 2 bits de la clave son distinto para ambos (fondo amarillo).

Clave Alice	1	0	0	0	1	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1
Clave Bob	1	0	0	1	1	1	0	0	1	1	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1

6. Alice y Bob eligen aleatoriamente la mitad de la cadena obtenida y las comparan vía un canal clásico. En el ejemplo se eligen 12 bits para comparar (columnas sombreadas de celeste).

Clave Alice	1	0	0	0	1	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1
Calve Bob	1	0	0	1	1	1	0	0	1	1	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1

7. Al comparar Alice y Bob estiman el valor del QBER. Si hay más diferencias que un límite fijado de antemano se reinicia el protocolo. En el ejemplo QBER=1/12=8.3%.

Alice	0	1	0	0	1	0	0	0	1	1	1	1
Bob	0	1	0	1	1	0	0	0	1	1	1	1

8. Si las diferencias son menores que el límite fijado se procede a la corrección de errores, hasta que no encuentren diferencias en los bloques analizados. Luego de corregir se obtiene claves iguales para Alice y Bob.

9. Luego de la corrección de errores se procede a amplificar la privacidad para reducir la cantidad de información de un posible espía.

10. Finalmente lo que queda de la cadena es la clave, común para ambos.

Longitud de la clave de Alice y Bob

La Figura 14 muestra visualmente como se estima la longitud de la clave. Probabilísticamente la mitad de veces Bob acertará la base de envío de Alice por tanto sólo aproximadamente el 50% de los fotones enviados servirán para formar la clave.

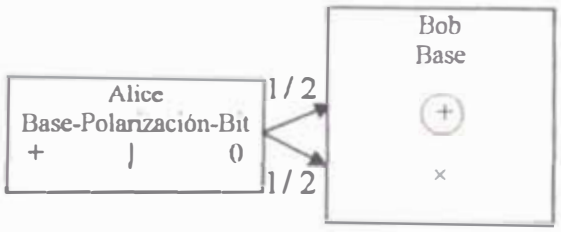


Figura 14: Probabilísticamente la mitad de veces Bob acertará la base de Alice y esta será considerada para formar la clave común.

Analicemos esquemáticamente cada posibilidad (Figura 15).

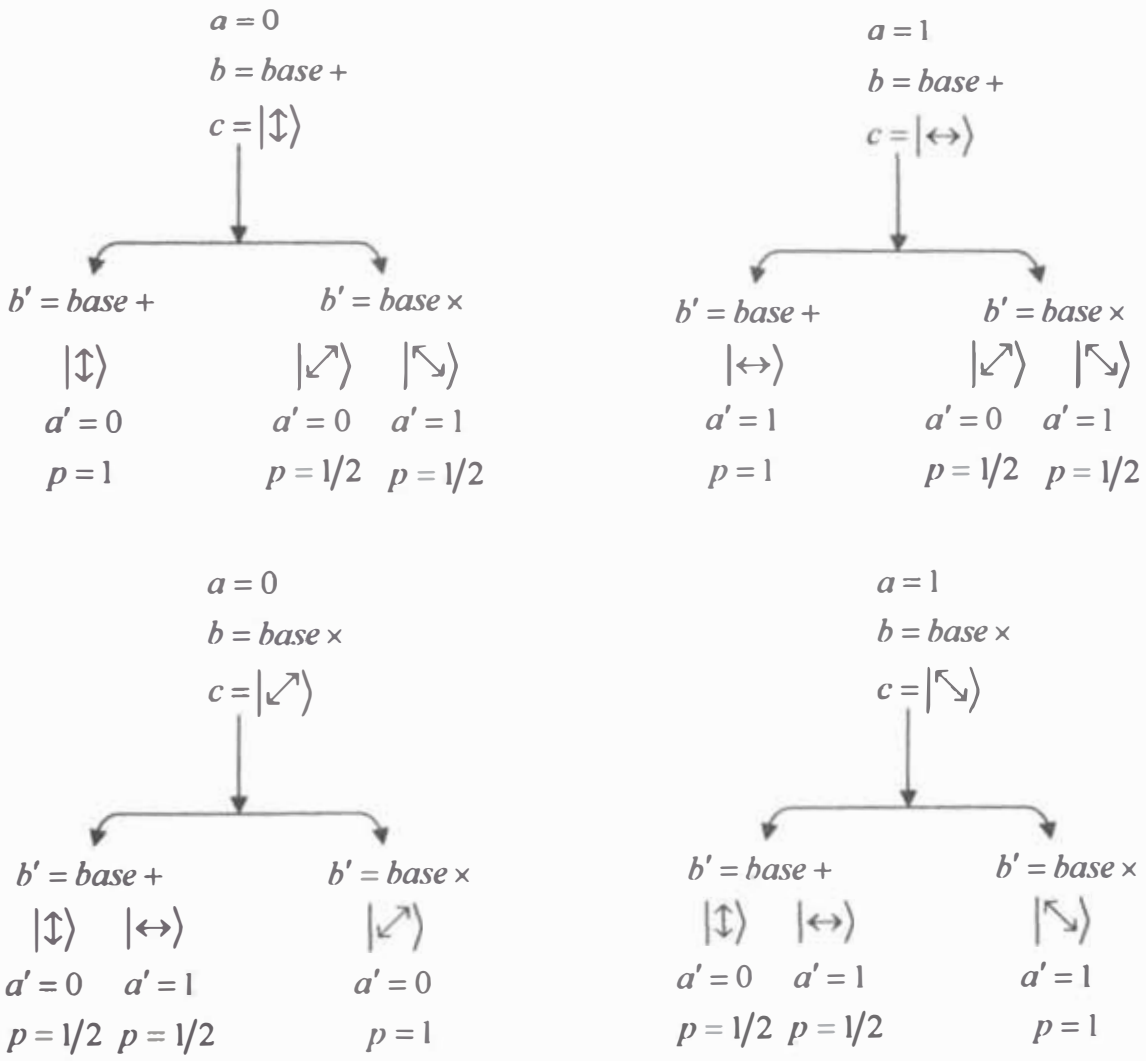


Figura 15: Medidas posibles durante la ejecución del protocolo.

2.3.1.2 Cálculo de probabilidades de acierto y error en la transmisión

La comunicación segura entre Alice y Bob está expuesta a alteraciones producidas tanto por intervención de espías como por el ruido presente en la línea de transmisión (canal cuántico). No debemos confundir el error del ruido con el error ocasionado por un espía, la diferencia radica en que el espía siempre tratará en lo posible de enviar la polarización original después de medirlo. En cambio el ruido cambia de todas formas la polarización del fotón afectado y por tanto el error debido al ruido puede ser mayor. En lo que sigue se discutirá varios casos, los mismos que serán modelados.

A. Cálculo de probabilidades sin espías y sin ruido

Cuando no existe ruido ni espías Bob acierta el 100% de la clave de Alice (que está formada por aproximadamente por el 50% de los bits enviados por Alice). Es el caso ideal. En la Figura 16 se muestra visualmente los aciertos de Bob. El símbolo *V* significa que se obtuvo la polarización correcta.

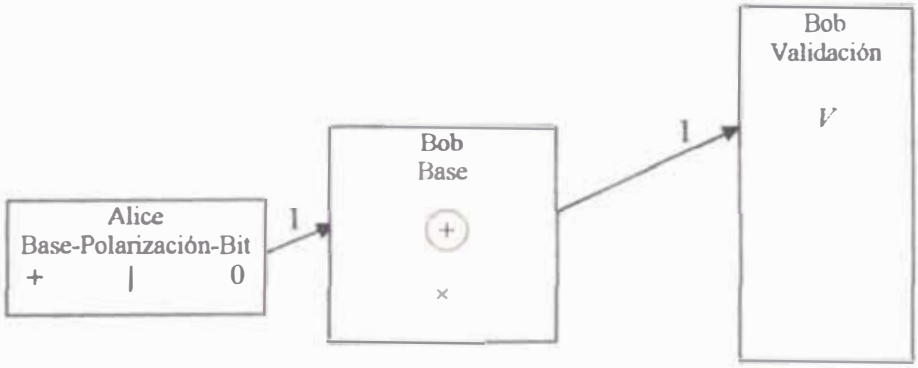


Figura 16: Transmisión sin espía y sin ruido.

De la Figura 16 tenemos:

$$\boxed{p_{acertar}^{Bob} = 1 = 100\%} \quad \cdots(1)$$

$$\boxed{p_{equivocar}^{Bob} = 0\%} \quad \cdots(2)$$

Como el QBER es el error cometido en la clave de Bob entonces:

$$\boxed{QBER = 0\%} \quad \cdots(3)$$

B. Cálculo de probabilidades con un espía de intervención máxima y sin ruido

Este caso se presenta cuando el espía Eve interviene cada fotón enviado por Alice y luego reenvía a Bob en la polarización medida por ella. Así se produce el máximo error al construir la clave por parte de Bob

En la Figura 17 se muestra visualmente como se produce el error máximo que ocasiona un espía que interviene cada fotón que forma la clave. El símbolo *V* significa que se obtuvo la polarización correcta y el símbolo *X* que se equivoco. Probabilísticamente el 50% de las veces el espía acierta la base y no modifica la polarización del fotón, por tanto la presencia del espía no modifica el fotón que llega a Bob. En el otro 50% no acierta la base y modifica la polarización del fotón Entonces al llegar este fotón a Bob, existe el 50% de probabilidad de que colapse en la polarización original de Alice, es decir un 25% y el otro 25% estará en la polarización ortogonal. En total Bob tendrá probablemente el 75% de bits correctos y 25% incorrectos

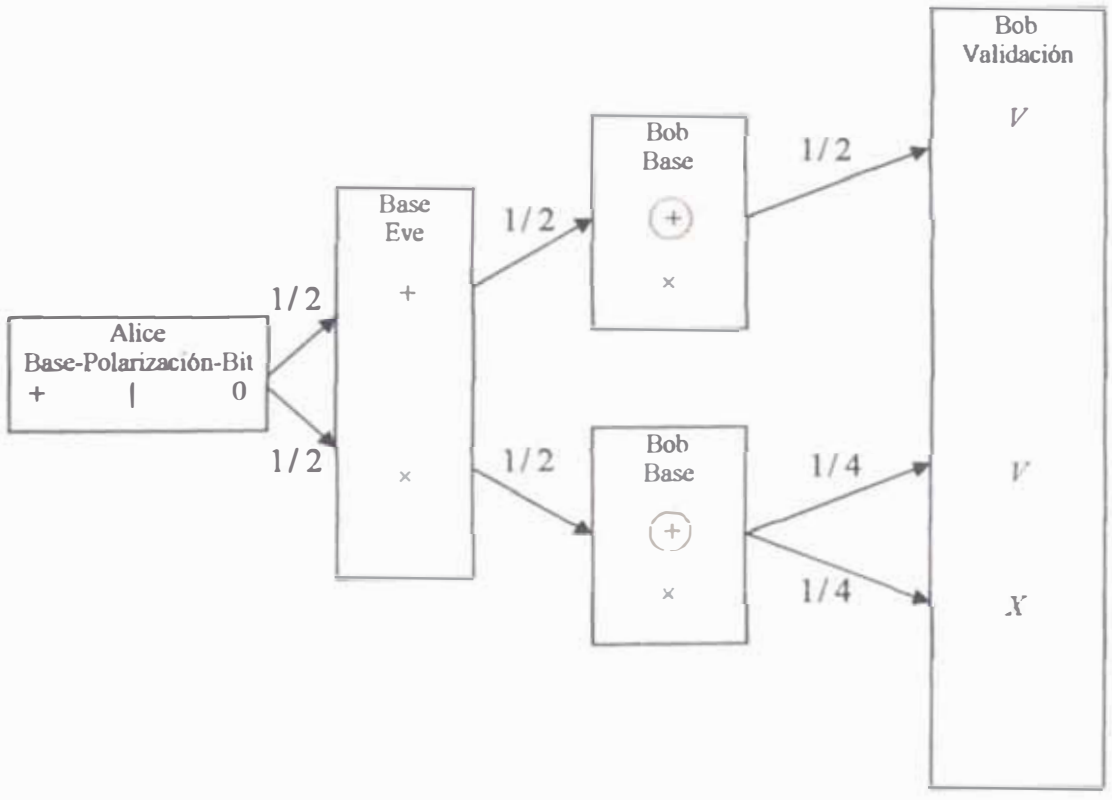


Figura 17: Transmisión sin ruido y con espía que intercepta todos los fotones.

En conclusión tenemos:

$$p_{acertar}^{Bob} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4} = 75\% \quad \cdots(4)$$

$$\boxed{p_{equivocar}^{Bob} = \frac{1}{4} = 25\%} \quad \cdots(5)$$

$$\boxed{QBER = 25\%} \quad \cdots(6)$$

¿Cuánto acierta Eve en este caso?

Aproximadamente el 50% de veces Eve acierta en la elección de la base y por tanto acierta la polarización y por tanto los bits correspondientes. Del otro 50% sólo le queda adivinar y acertará la mitad de los bits, es decir que el 25% lo acierta por suerte. En total se espera que Eve acierte con probabilidad un 75% y se equivoque en un 25%.

$$\boxed{p_{acertar}^{Eve} = \frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4} = 75\%} \quad \cdots(7)$$

$$\boxed{p_{equivocar}^{Eve} = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4} = 25\%} \quad \cdots(8)$$

C. Cálculo probabilidades en un ataque parcial de probabilidad λ sin ruido

Ahora, es posible que el espía solo ataque parcialmente, es decir cada fotón tiene la probabilidad λ, $0 \leq \lambda \leq 1$, de ser atacado y una probabilidad $1-\lambda$ de no ser atacado. El ataque máximo sucede cuando $\lambda = 1$. Analicemos varios casos:

Según las ecuaciones 1 y 2, en la parte no atacada Bob tiene la probabilidad de acertar:

$$p_{acertar}^{Bob} = (1-\lambda) \quad \cdots(9)$$

Y de equivocarse:

$$p_{equivocar}^{Bob} = 0 \quad \cdots(10)$$

Según las ecuaciones 4 y 5, en la parte atacada Bob tiene las probabilidades:

$$p_{acertar}^{Bob} = \frac{3\lambda}{4} \quad \cdots(11)$$

$$p_{equivocar}^{Bob} = \frac{\lambda}{4} \quad \cdots(12)$$

En conclusión, de (9) y (11) la probabilidad total de acierto es:

$$\boxed{p_{acertar}^{Bob} = (1-\lambda) + \frac{3}{4}\lambda = 1 - \frac{\lambda}{4}} \quad \cdots(13)$$

Y de (10) y (12) la probabilidad de equivocarse Bob es:

$$\boxed{p_{equivocar}^{Bob} = \frac{\lambda}{4}} \quad \cdots(14)$$

$$\boxed{QBER = \frac{\lambda}{4}} \quad \cdots(15)$$

¿Cuánto acierta Eve en este caso?

Eve ataca con una probabilidad λ entonces en la parte atacada (ver ecuación 7) la probabilidad de acierto de Eve es:

$$p_{acertar}^{Eve} = \frac{3\lambda}{4} \quad \cdots(16)$$

Y de no acertar (ver ecuación 8) es:

$$p_{equivocar}^{Eve} = \frac{\lambda}{4} \quad \cdots(17)$$

Y en la parte que no ataca sólo le queda adivinar acertando con probabilidad un 50%, es decir (1-λ)/2.

$$p_{acertar}^{Eve} = \frac{(1-\lambda)}{2} \quad \cdots(18)$$

$$p_{equivocar}^{Eve} = \frac{(1-\lambda)}{2} \quad \cdots(19)$$

En conclusión, de (16) y (18) la probabilidad total de acierto de Eve es:

$$\boxed{p_{acertar}^{Eve} = \frac{3}{4}\lambda + \frac{(1-\lambda)}{2} = \frac{1}{2} + \frac{\lambda}{4}} \quad \cdots(20)$$

Y de (17) y (19) la probabilidad de equivocarse es:

$$p_{equivocar}^{Eve} = \frac{\lambda}{4} + \frac{(1-\lambda)}{2} = \frac{1}{2} - \frac{\lambda}{4} \quad \cdots(21)$$

D. Cálculo de probabilidades debido a un ruido δ% sin espía

El ruido ocasiona que el bit afectado cambie su polarización. Si cambia a la polarización ortogonal se producirá un error seguro, pero si cambia a una polarización correspondiente a otra base entonces tiene un 50% de probabilidad de causar un error. Todo depende del estado en que colapse el fotón.

En la Figura 18 se muestra visualmente el porcentaje de error que se obtiene en los bits afectados por ruido caracterizado por el factor δ%. Un bit codificado en la polarización $|\updownarrow\rangle$ tiene sólo 1/3 de probabilidad de cambiar a la polarización ortogonal $|\leftrightarrow\rangle$ y causar un error, los otros 2/3 corresponden a cambiar a polarizaciones de la base diagonal ×. Cada uno acertará en un 50%, es decir en 1/6, entonces el error total es 1/3+1/6+1/6=2/3, es decir que un ruido de δ% ocasiona un error en la clave de Bob de 2/3 δ%.

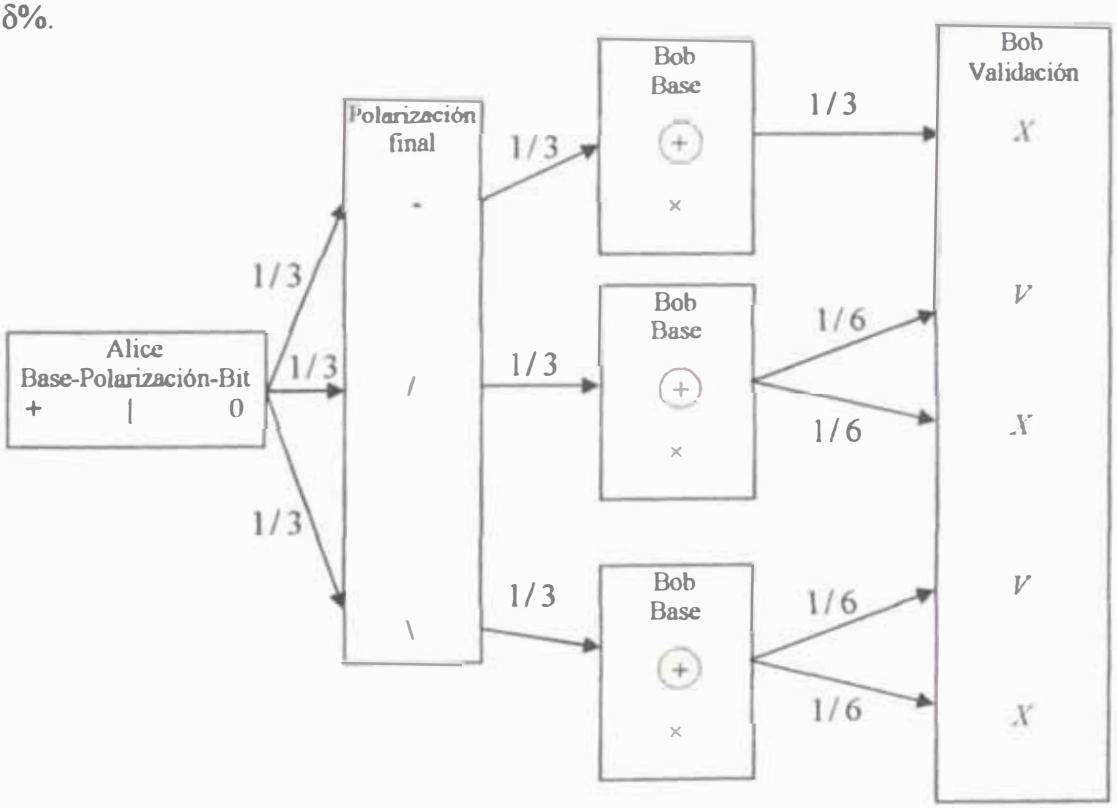


Figura 18: Un ruido de δ% ocasiona un error probable en la clave de Bob de 2/3 δ%.

La Figura 18 muestra los porcentajes del δ% afectado:

$$p_{acertar}^{Bob} = \frac{2}{6}\delta\% = \frac{1}{3}\delta\% \quad \cdots(22)$$

$$p_{equivocar}^{Bob} = \frac{1}{3}\delta\% + \frac{2}{6}\delta\% = \frac{2}{3}\delta\% \quad \cdots(23)$$

Y del (100-δ)% que no es afectado por el ruido se tiene (ver ecuación 1 y 2):

$$p_{acertar}^{Bob} = (100-\delta)\% \quad \cdots(24)$$

$$p_{equivocar}^{Bob} = 0 \quad \cdots(25)$$

En conclusión, de (22) y (24), la probabilidad de acertar de Bob es:

$$\boxed{p_{acertar}^{Bob} = \frac{1}{3}\delta\% + (100-\delta)\% = \left(100 - \frac{2}{3}\delta\right)\%} \quad \cdots(26)$$

Y de (23) y (25), la probabilidad de equivocarse es:

$$\boxed{p_{equivocar}^{Bob} = \frac{2}{3}\delta\%} \quad \cdots(27)$$

$$\boxed{QBER = \frac{2}{3}\delta\%} \quad \cdots(28)$$

E. Cálculo de probabilidades debido a un ruido δ% con ataque parcial de probabilidad λ

Se tiene tres posibilidades de que el ruido afecte a la polarización del fotón:

1. **Ruido antes de que Eve mida**: En este caso Eve recibe un fotón con polarización cambiada, lo mide y tiene un 50% de cambiar su base, lo que significa modificar nuevamente la polarización del fotón, pero en resumen se puede decir que el fotón solo tuvo un cambio, desde su polarización inicial hasta la polarización obtenida por Eve. Luego Eve reenvía el fotón resultante con una polarización conocida por ella, lo que le da información al momento de construir su clave, pues conoce la polarización que recibe Bob.
2. **Ruido después de que Eva mida**: En este caso Eve recibe un fotón con polarización correcta, lo mide y tiene un 50% de cambiar su base, reenvía el fotón con una polarización conocida por ella, pero el ruido cambia esta polarización y pierde esta información reduciendo la probabilidad de acertar el bit, pues ahora no conoce la polarización que recibe Bob.

3. **Ruido antes y después de que Eva mida**: En este caso Eve recibe un fotón con polarización cambiada, lo mide y tiene un 50% de cambiar su base, lo que significa modificar nuevamente la polarización del fotón, pero en resumen se puede decir que el fotón solo tuvo un cambio, desde su polarización inicial hasta la polarización obtenida por Eve. Luego Eve reenvía el fotón resultante con una polarización conocida por ella, pero el ruido cambia esta polarización y pierde esta información reduciendo la probabilidad de acertar el bit, pues ahora no conoce la polarización que recibe Bob

De los tres casos, sólo en el primero Eve tiene información para poder aumentar su probabilidad de deducir la clave, conoce la polarización que recibe Bob, pero en los otros dos casos Eve pierde esta información pues el ruido cambia nuevamente la polarización.

Por tanto es en el primer caso donde Eve tiene más probabilidad de conocer la clave, por eso en esta tesis sólo se analiza este caso pues si el protocolo asegura que Eve no puede deducir la clave entonces se habrá comprobado que el protocolo es seguro.

De los bits que no son afectados por el ruido, (100-δ)%, es posible que sean intervenidos por Eve con una probabilidad λ entonces de la ecuación 11, Bob tiene la probabilidad de acertar:

$$p_{acertar}^{Bob} = \frac{3}{4}\lambda(100-\delta)\% = \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% \quad \cdots(29)$$

Y de la ecuación 12, Bob tiene la probabilidad de equivocarse:

$$\boxed{p_{equivocar}^{Bob} = \frac{1}{4}\lambda(100-\delta)\% = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\%} \quad \cdots(30)$$

De los bits que no son afectados por el ruido (100-δ)% se tiene una probabilidad de (1-λ) que no sean interceptados por el espía entonces de la ecuación 1, Bob acierta con una probabilidad:

$$\left|p_{acertar}^{Bob} = (1-\lambda)(100-\delta)\% = (100-\delta-100\lambda+\lambda\delta)\%\right| \quad \cdots(31)$$

Y de la ecuación 2, Bob se equivoca con una probabilidad:

$$\boxed{p_{equivocar}^{Bob} = 0} \quad \cdots(32)$$

De los bits que son afectados por el ruido, δ%, estos son intervenidos por Eve con una probabilidad λ y es posible que algunos regresen a su polarización original. En la Figura 19 se muestra el análisis. Se observa que en 5/12 casos acierta y en 1/6 + 5/12 = 7/12 casos comete error.

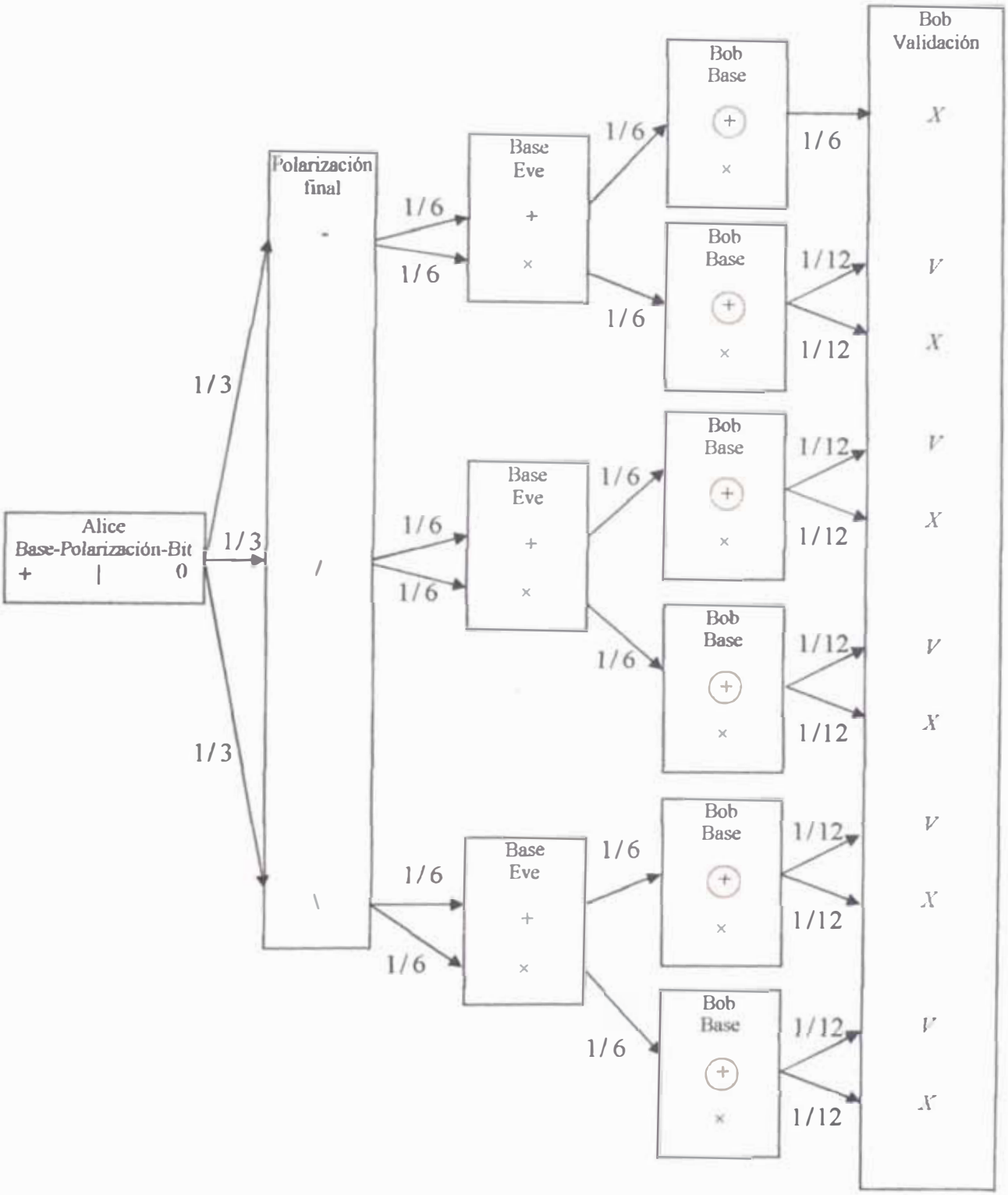


Figura 19: El espía interviene con una probabilidad λ. La parte de la clave de Bob afectada por el ruido δ% tiene un error de 7δ/12 %.

De la Figura 19, tenemos que Bob acierta:

$$p_{acertar}^{Bob} = \frac{5}{12}\lambda\delta\% \quad \cdots(33)$$

Y se equivoca:

$$p_{equivocar}^{Bob} = \frac{7}{12}\lambda\delta\% \quad \cdots(34)$$

Pero además, el (1-λ) del δ% que no es intervenido por Eve, solo es afectado por el ruido y se tendrá según la ecuación 22 un acierto de *1/3*:

$$p_{acertar}^{Bob} = \frac{1}{3}(1-\lambda)\delta\% = \left(\frac{1}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(35)$$

Y según la ecuación 23 un error del 2/3:

$$p_{equivocar}^{Bob} = \frac{2}{3}(1-\lambda)\delta\% = \left(\frac{2}{3}\delta - \frac{2}{3}\lambda\delta\right)\% \quad \cdots(36)$$

En conclusión, de (29), (31), (33) y (35), Bob acierta con probabilidad:

$$\begin{aligned} p_{acertar}^{Bob} &= \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% + (100 - \delta - 100\lambda + \lambda\delta)\% + \frac{5}{12}\lambda\delta\% + \left(\frac{1}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \\ &= \left(100 - \frac{2}{3}\delta - 25\lambda + \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(37)$$

Y de (30), (32), (34) y (36), Bob se equivoca con probabilidad:

$$p_{equivocar}^{Bob} = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% + 0 + \frac{7}{12}\lambda\delta\% + \left(\frac{2}{3}\delta - \frac{2}{3}\lambda\delta\right)\% = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(38)$$

$$QBER = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(39)$$

¿Cuánto acierta Eve en este caso?

De los bits no afectados por el ruido (100-δ)%, es probable que sean atacados con una probabilidad λ entonces de la ecuación 16, Eve acierta·

$$p_{acertar}^{Eve} = \frac{3}{4}\lambda(100-\delta)\% = \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% \quad \cdots(40)$$

Y de la ecuación 17, Eve se equivoca:

$$p_{equivocar}^{Eve} = \frac{1}{4}\lambda(100-\delta)\% = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% \quad \cdots(41)$$

De los bits no afectados por el ruido (100-δ)%, es probable que el (1-λ) no sean atacados, entonces a Eve sólo le queda adivinar y acierta los bits con una probabilidad del 50%:

$$p_{acertar}^{Eve} = \frac{1}{2}(1-\lambda)(100-\delta)\% = \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% \quad \cdots(42)$$

$$p_{equivocar}^{Eve} = \frac{1}{2}(1-\lambda)(100-\delta)\% = \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% \quad \cdots(43)$$

De los bits que son afectados por el ruido δ%, existe la probabilidad λ de ser espiados, este caso se analiza en la Figura 20.

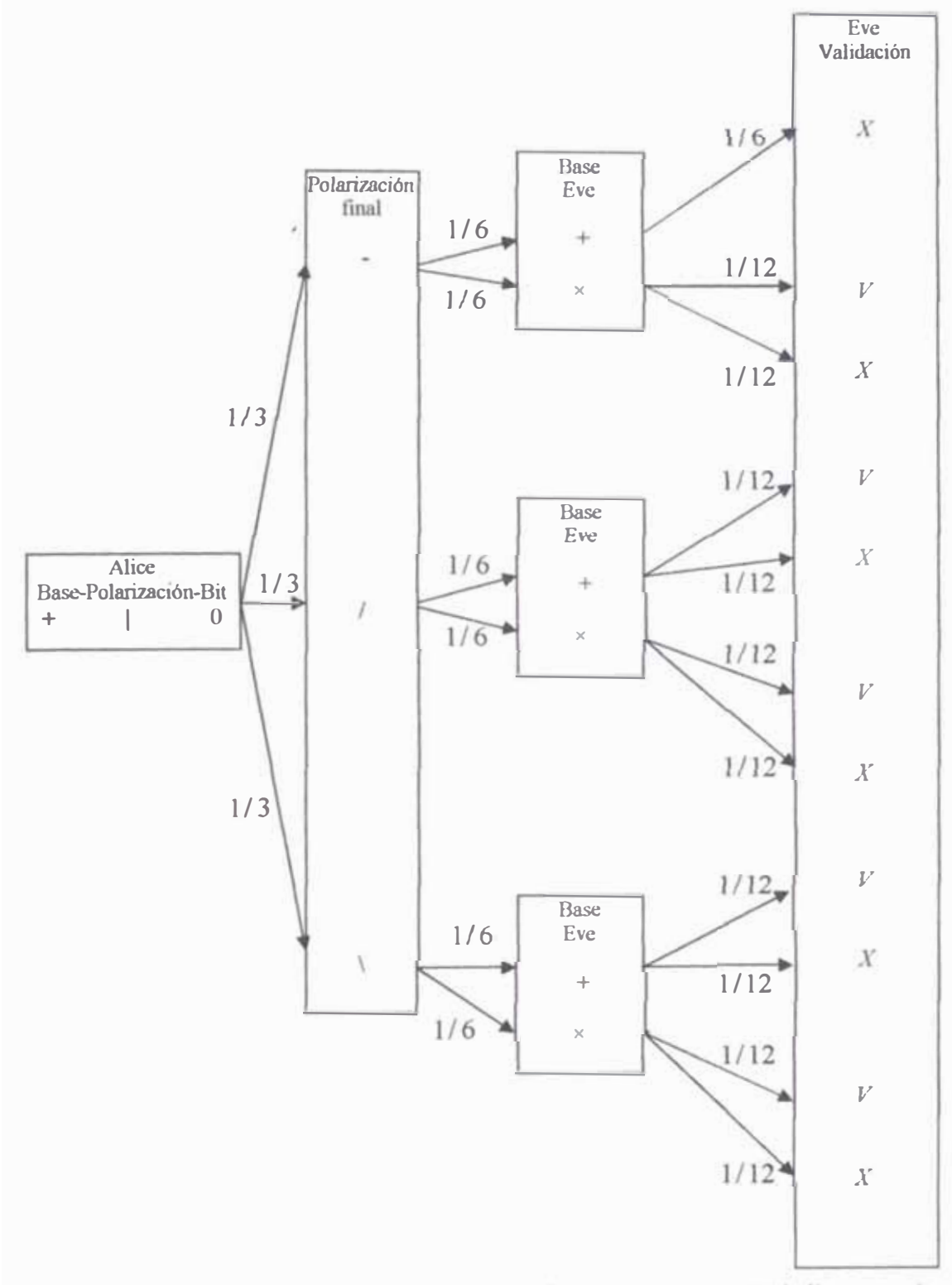


Figura 20: El espía interviene con una probabilidad 2. La parte de la clave de Eve afectada por el ruido 6% tiene un acierto de 52.6/12 %.

En la Figura 20 se observa que en un solo caso se puede asegurar con certeza que Eve se equivocará, los otros casos son inciertos y tiene un 50% de acertar o equivocarse, por tanto obtenemos:

$$p_{acertar}^{Eve} = \frac{5}{12}\lambda\delta\% \quad \cdots(44)$$

$$p_{equivocar}^{Eve} = \left(\frac{1}{6}\lambda\delta + \frac{5}{12}\lambda\delta\right)\% = \frac{7}{12}\lambda\delta\% \quad \cdots(45)$$

De los bits que son afectados por el ruido δ%, existe la probabilidad (1-λ)δ% que no sean espiados, entonces a Eve sólo le queda adivinar y acierta los bits con una probabilidad del 50%:

$$p_{acertar}^{Eve} = \frac{1}{2}(1-\lambda)\delta\% = \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \quad \cdots(46)$$

$$p_{equivocar}^{Eve} = \frac{1}{2}(1-\lambda)\delta\% = \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \quad \cdots(47)$$

En conclusión, de (40), (42), (44) y (46) Eve tiene una probabilidad de acertar:

$$\begin{aligned} p_{acertar}^{Eve} &= \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% + \left(50 - \frac{\delta}{2} - 50\lambda + \frac{\lambda\delta}{2}\right)\% + \frac{5}{12}\lambda\delta\% + \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \\ &= \left(50 + 25\lambda - \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(48)$$

Y de (41), (43), (45) y (47) Eve tiene una probabilidad de equivocarse:

$$\begin{aligned} p_{equivocar}^{Eve} &= \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% + \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% + \frac{7}{12}\lambda\delta\% + \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \\ &= \left(50 - 25\lambda + \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(49)$$

2.3.1.3 Resumen de las fórmulas probabilísticas que describen el protocolo cuántico BB84

Se muestra a continuación un resumen de las fórmulas probabilísticas de acierto y error en cualquier situación (ruido y espía) de envío de fotones en el protocolo BB84, previas a las etapas de reconciliación de información y la amplificación de privacidad que se efectúan independientemente al terminar la transmisión por el canal clásico. Se debe resaltar que la deducción de estas fórmulas y las fórmulas mismas no están publicadas en medios conocidos y es quizás también un aporte de esta tesis.

Para un sistema afectado por un ruido de δ% y bajo un ataque de un espía con capacidad de interceptación λ, se tiene los siguientes resultados:

De la ecuación 37, se tiene que la probabilidad que cada bit de la clave de Bob sea igual al bit de la clave de Alice es:

$$p_{acierto}^{Bob} = \left(100 - \frac{2}{3}\delta - 25\lambda + \frac{1}{3}\lambda\delta\right)\% \quad \cdots(I)$$

De la ecuación 38, la probabilidad que cada bit de la clave de Bob sea diferente al bit de la clave de Alice es:

$$p_{equivocar}^{Bob} = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(II)$$

De la ecuación 40, la tasa de error de bits cuánticos (QBER) entre las claves de Alice y Bob es:

$$QBER = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(III)$$

En el lado del espía, de la ecuación 48, la probabilidad que cada bit de la clave de Eve sea igual al bit de la clave de Alice es:

$$p_{acierto}^{Eve} = \left(50 + 25\lambda - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(IV)$$

Y de la ecuación 49, la probabilidad que cada bit de la clave de Eve sea diferente al bit de la clave de Alice es:

$$\boxed{p_{equivocar}^{Eve} = \left(50 - 25\lambda + \frac{1}{3}\lambda\delta\right)\%} \quad \cdots(V)$$

Aplicando estas fórmulas a algunos casos específicos tenemos:

a. Con un ruido δ% y sin espía (λ=0), reemplazando en las ecuaciones I, II, III, IV y V se obtiene las mismas ecuaciones que se dedujo en el párrafo 2.3.1.2, apartado D:

Aciertos de Bob:

$$p_{acertar}^{Bob} = \left(100 - \frac{2}{3}\delta\right)\%$$

que es igual a la ecuación (26).

Errores de Bob:

$$p_{equivocar}^{Bob} = \left(\frac{2}{3}\delta\right)\%$$

que es igual a la ecuación (27).

QBER:

$$QBER = \left(\frac{2}{3}\delta\right)\%$$

que es igual a la ecuación (28).

Aciertos de Eve: Como Eve no interviene entonces sólo le queda elegir aleatoriamente entre los bit 0 y 1, acertando probabilísticamente el 50%, qué es lo que refleja el resultado obtenido.

$$p_{acertar}^{Eve} = (50)\%$$

Errores de Eve: De acuerdo a lo indicado antes, Eve se equivoca el 50%.

$$p_{equivocar}^{Eve} = (50)\%$$

b. Otro ejemplo, en el caso donde no existe ruido (δ=0) con un espía de interceptación λ, ~~reemplazando~~ en las ecuaciones *I*, *II*, *III*, IV y V obtenemos las mismas ecuaciones que deducimos en el párrafo 2.3.1.2, apartado C:

Aciertos de Bob:

$$p_{acertar}^{Bob} = (100 - 25\lambda)\% = 1 - \frac{1}{4}\lambda$$

que es igual a la ecuación (13).

Errores de Bob:

$$p_{equivocar}^{Bob} = (25\lambda)\% = \frac{\lambda}{4}$$

que es igual a la ecuación (14).

QBER:

$$QBER = (25\lambda)\% = \frac{\lambda}{4}$$

que es igual a la ecuación (15).

Aciertos de Eve:

$$p_{acertar}^{Eve} = (50 + 25\lambda)\% = \frac{1}{2} + \frac{\lambda}{4}$$

que es igual a la ecuación (20).

Errores de Eve:

$$p_{equivocar}^{Eve} = (50 - 25\lambda)\% = \frac{1}{2} - \frac{\lambda}{4}$$

que es igual a la ecuación (21).

PARTE II

TRABAJO EXPERIMENTAL

En medio de muy limitados recursos económicos disponibles, se diseño y construyó una máquina experimental de criptografía simplificada a lo esencial respecto a equipos modernos desarrollados en laboratorios más avanzados Algunos de estos desarrollos modernos se presentan en el Capítulo 3. Se demuestra en esta Parte II del trabajo que esta máquina produce los mismos resultados básicos que una moderna En el Capitulo 4 se presenta la deducción de las fórmulas probabilísticas que gobiernan el funcionamiento de la máquina construida mostrando que estas fórmulas son equivalentes a las deducidas para las máquinas modernas En el Capítulo 5 se describe la simulación computarizada completa de la generación de la clave cuántica en el marco del protocolo BB84 con la finalidad de comparar los resultados con las fórmulas probabilísticas antes mencionadas, habiendo una razonable coincidencia. En el Capítulo 6 se resume las características y el funcionamiento de una primera versión de máquina de criptografía cuántica Finalmente, en el Capítulo 7, se describen varios experimentos que se efectuaron para comprobar el protocolo cuántico BB84 analizando los resultados experimentales obtenidos

Como consecuencia de esta experiencia teórico-práctico en criptografía, en el Capítulo 8 se presenta una propuesta de diseño futuro de una máquina de criptografía cuántica factible de ser realizado en nuestro medio con recursos económicos accesibles.

Capítulo 3

Introducción

El trabajo experimental realizado en esta tesis consta de tres partes relacionadas:

1. Deducción de las fórmulas probabilísticas que gobiernan la máquina que construimos.

   En el párrafo 2.3.1.2 se dedujo las fórmulas probabilísticas que gobiernan una máquina moderna, mediante un análisis similar en nuestra máquina se encuentran las mismas fórmulas.

2. Simulación en computadora clásica del protocolo cuántico BB84 utilizando el diseño de nuestra máquina y comparación con las fórmulas teóricas.

   Al no tener un equipo real para realizar el experimento, la simulación por computadora ofrece una oportunidad de asegurarnos que el diseño de la máquina es correcto. Se obtuvieron resultados que coinciden con las predicciones teóricas.

3. Construcción de un equipo experimental que aplique el protocolo cuántico BB84.

   Esta es la culminación del trabajo experimental donde comprobamos en la realidad que el protocolo BB84 funciona en nuestra máquina. Debe resaltarse que la máquina construida en esta tesis es un diseño simplificado y único que surge como una necesidad de salvar obstáculos económicos.

3.1 Antecedentes de trabajos similares

Esta es una primera prueba en el Perú para desarrollar la Criptografía Cuántica. A este respecto es apropiado mencionar que en esta primera década del siglo XXI se están desarrollando trabajos experimentales de criptografía cuántica en varias universidades e instituciones científicas en todo el mundo. Ellos nos sirven de guía para la construcción de nuestro prototipo obviamente dentro de las grandes limitaciones financieras y técnicas de nuestro medio.

A continuación se presenta como referencia algunas tesis experimentales que describen desarrollos de criptografía cuántica a través del aire libre o en fibra óptica, usando protocoles basados en estados ortogonales o estados entrelazados:

- "On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source" por Chris Erven. Universidad de Waterloo. Tesis para optar el grado de Maestría en Ciencias Físicas (2007). Genera fotones entrelazados mediante la Conversión Paramétrica Espontanea Descendente (Spontaneous Parametric Down Conversion) e implementa el protocolo BBM92, distribuyendo una clave cuántica por aire en zona urbana a una distancia de 580 m (30)

- "Long distance free-space quantum key distribution" por Tobias Schmitt-Manderbach Universidad Ludwig–Maximilians de Munich. Tesis de Doctor en Física (2007) Genera fotones individuales mediante láseres atenuados e implementa el protocolo BB84 logrando distribuir una clave cuántica por aire a una distancia de 144 km (31).

- "Experimental Quantum Cryptography" por Henning Weier. Universidad Técnica de Munich. Tesis de Diplomado en Física (2003). Genera fotones individuales mediante láseres atenuados e implementa del protocolo BB84 para distribuir una clave cuántica por aire en zona urbana a una distancia de 0.5 Km (32).

- "Experimental Quantum Cryptography" por Martin Hendrych. Universidad de Olomouc, República Checa Tesis para optar el grado de Doctor en Física (2002). Genera fotones individuales mediante un laser atenuado e implementa el protocolo

BB84 para distribuir una clave cuántica por fibra óptica a una distancia de 0.5 Km (33).

- "Quantum cryptography and quantum cryptanalysis" por Vadim Makarov. Universidad Noruega de Ciencia y Tecnología. Tesis para optar el grado de Doctor en Ingeniería (2007). Genera fotones individuales mediante láseres atenuados e implementa el protocolo BB84 para distribuir una clave cuántica por fibra óptica dentro de un laboratorio (34).

- "Advanced Techniques in Free Space Quantum Communication" por Ivan Capraro. Universidad de Padova, Italia. Tesis para optar el grado de Doctor en Ingeniería de la Información (2008). Genera fotones individuales mediante láseres atenuados e implementa el protocolo B92 para distribuir una clave cuántica a 100 m. en aire libre (35).

Capítulo 4

Deducción de las fórmulas probabilísticas en la transmisión de la clave

Para poder deducir correctamente las fórmulas probabilísticas que gobiernan el funcionamiento de nuestra máquina debemos tener en cuenta que la gran diferencia de diseño entre la máquina moderna y la construida es el sistema de medida de Bob. En el diseño moderno el sistema de medida de Bob cuenta con un beamsplitter no polarizador, dos beamsplitters polarizadores, una lámina retardadora media onda y cuatro detectores fotodiodos de avalancha En cambio nuestra máquina reemplaza todo esto por un disco giratorio con cuatro polarizadores y un fototransistor. Esta simplificación extrema conlleva a un análisis diferente de probabilidades de acierto y error en la clave de Bob y Eve que se irá explicando a medida que analicemos cada caso.

Otra diferencia importante es que en la máquina convencional Alice utiliza una fuente de fotones individuales, en cambio nuestra máquina utiliza pulsos de fotones, sin embargo en la simulación se puede programar fotones individuales.

El objetivo del presente párrafo es comprobar que las probabilidades de error y acierto de nuestra máquina son iguales a la de la máquina convencional y así concluir que ambas máquinas son completamente equivalentes. En el párrafo 2.3.1.2 se encuentran los cálculos de probabilidades de la máquina convencional.

Longitud de la clave de Alice y Bob

La máquina construida, por falta de presupuesto, no usa beamsplitters, por tanto no se puede hacer un análisis a nivel de base como en la máquina convencional, la máquina utiliza directamente polarizaciones elegidas al azar con lo que el error en detectar el bit correcto en la base correcta aumenta al 50% (en lugar del 0% del caso con beamsplitters), pero se puede corregir aplicando la siguiente regla: ***"si se mide cero entonces significa que se bloqueo la polarización de Alice y entonces la polarización correcta es la ortogonal"*** y el error regresa nuevamente a 0%, en nuestra máquina esta regla funciona porque siempre llegan fotones al polarizador de Bob, pues la distancia es corta y además porque en cada pulso se envía muchos fotones.

En la Figura 21 se muestra el análisis para calcular la longitud de la clave de Alice y Bob. Resulta el 50%, exactamente igual a la máquina convencional, párrafo 2.3.1.1.

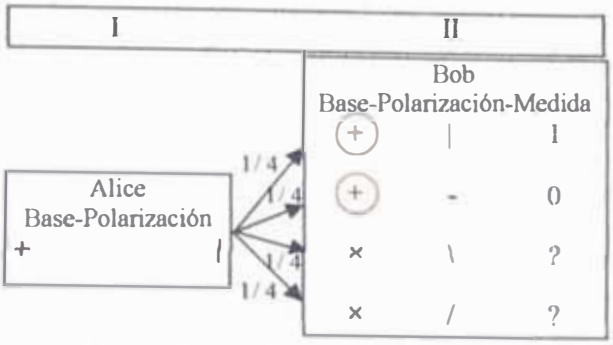


Figura 21: La longitud de la clave es la mitad de la longitud de fotones enviados.

Paso I: Alice elije una de las dos bases, por ejemplo + y una de las dos polarizaciones posibles, por ejemplo |.

Paso II: Bob elije una polarización para medir que corresponde a la base + o ×

Paso III: Bob solo toma en cuenta las bases que coinciden con Alice, vemos que de las 4 posibilidades puede acertar 2 (en círculo rojo), por tanto tiene una probabilidad de acertar de 2/4 = 50%.

Este resultado coincide con el de la máquina convencional y fue comprobado experimentalmente por nuestra máquina.

4.1 Cálculo de probabilidades sin espía y sin ruido

Alice y Bob sólo toman en cuenta las bases coincidentes para formar su clave, en este ejemplo Alice envía en la base + por tanto el bit sólo se tomará en cuenta cuando Bob mida con la base +. El análisis se muestra en la Figura 22.

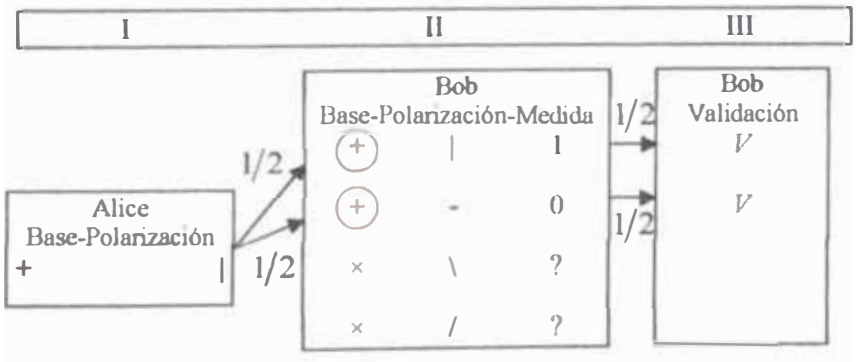


Figura 22: Obtención de la clave de Bob bajo un ataque sin intruso. *V*: Medida correcta

Paso I: Alice elije una de las dos bases, por ejemplo + y una de las dos polarizaciones posibles, por ejemplo |

Paso II: Alice y Bob sólo toman en cuenta las bases coincidentes en este caso +, en la mitad de esas bases coincidentes Bob acierta y mide 1. En la otra mitad no acierta y mide 0. En este punto acertó solo el 50%.

Paso III: Pero Bob sabe que si midió 0 entonces Alice envío la polarización ortogonal entonces deduce la polarización correcta, con lo que el 50% que estaba errado ahora se vuelve correcto.

En resumen las probabilidades de acierto y error de Bob:

$$\boxed{p_{acertar}^{Bob} = \frac{1}{2} + \frac{1}{2} = 100\%} \quad \cdots(51)$$

$$\boxed{p_{equivocar}^{Bob} = 0\%} \quad \cdots(52)$$

Como el QBER es el error cometido en la clave de Bob entonces:

$$\boxed{QBER = 0\%} \quad \cdots(53)$$

Este resultado coincide con el de la máquina convencional (ecuaciones 1, 2 y 3) y fue comprobado experimentalmente por nuestra máquina.

4.2 Cálculo de probabilidades con un espía de intervención máxima y sin ruido

No se cuenta con beamsplitters ni para Eve ni para Bob así que se usaron discos giratorios con polarizadores. En la Figura 23, se muestra el análisis en detalle. Bob interviene cada fotón de Alice y reenvía su resultado.

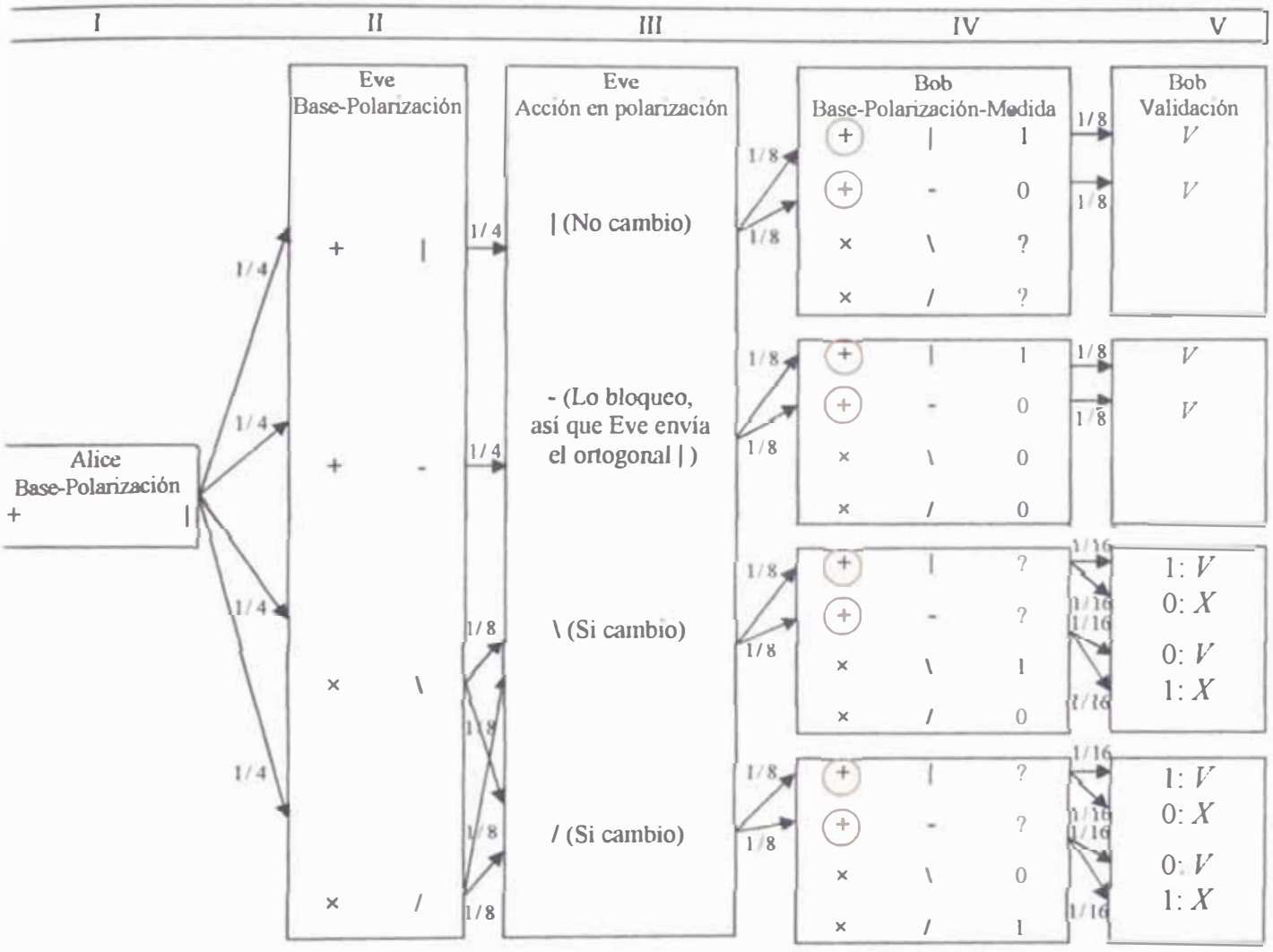


Figura 23: La máquina construida no tiene beamsplitters, el resultado que se obtiene es el mismo que la máquina convencional. El símbolo *V* significa que se obtuvo la polarización correcta y el símbolo *X* que se equivoco.

Paso I: Alice elije una de las 2 bases, por ejemplo + y una de las 2 polarizaciones posibles, por ejemplo |.

Paso II: Eve se decide por una de las 2 bases y elije una polarización posible, tiene 4 posibilidades.

Paso III: La intervención de Eve tiene un 25% de no cambiar la polarización, 25% de probabilidad de bloquear la señal, y 50% de cambiar de base. Eve reenvía la polarización que utiliza para medir excepto en el caso que lo bloquea, donde enviará la polarización ortogonal.

Paso IV: Bob elije una base, una polarización y mide. El 1 indica que si detecto señal, el 0 que no la detecto y la ? indica que no se puede saber de antemano si detectará o no, todo depende en qué estado colapse el fotón.

Es posible que ocurra una señal que parezca que no ha sido intervenida, en los caso "+, |, 1" ó "+, –, 0".

Expliquemos, si no hubiera intervención entonces la situación según el protocolo BB84 sería la siguiente:

- Alice envía +, |
- Si Bob utiliza +, | debe medir 1 y tomar en cuenta para formar la clave
- Si Bob utiliza +, – debe medir 0 y tomar en cuenta la polarización ortogonal para formar la clave
- Si Bob utiliza × no debe tomar en cuenta para formar la clave.

Paso V: Bob sólo tomará en cuenta su medida cuando su base ha sido +. En este caso se tiene 8 posibles situaciones en que ello sucede. Pero también se observa que de las 8 situaciones, solo en 4 no hubo rastro de alguna intervención (V). Entonces Bob obtiene una coincidencia segura en 4/8 = 50%.

Pero hay 4 casos donde los resultados son probabilísticos, que sólo aparentan que no hubo rastro de intervención con una probabilidad cada uno de 1/16.

En conclusión, las probabilidades de acierto y error de Bob:

$$p_{acertar}^{Bob} = \frac{4}{8} + \frac{4}{16} = \frac{3}{4} = 75\% \quad \cdots(54)$$

$$p_{equivocar}^{Bob} = \frac{4}{16} = \frac{1}{4} = 25\% \quad \cdots(55)$$

$$\boxed{QBER = 25\%} \quad \cdots(56)$$

Exactamente igual a los resultados encontrados en la máquina convencional, ecuaciones 4, 5 y 6.

¿Cuánto acierta Eve en este caso?

En la Figura 24 se muestra visualmente un ejemplo de cómo se calcula la probabilidad de que Eve obtenga la clave.

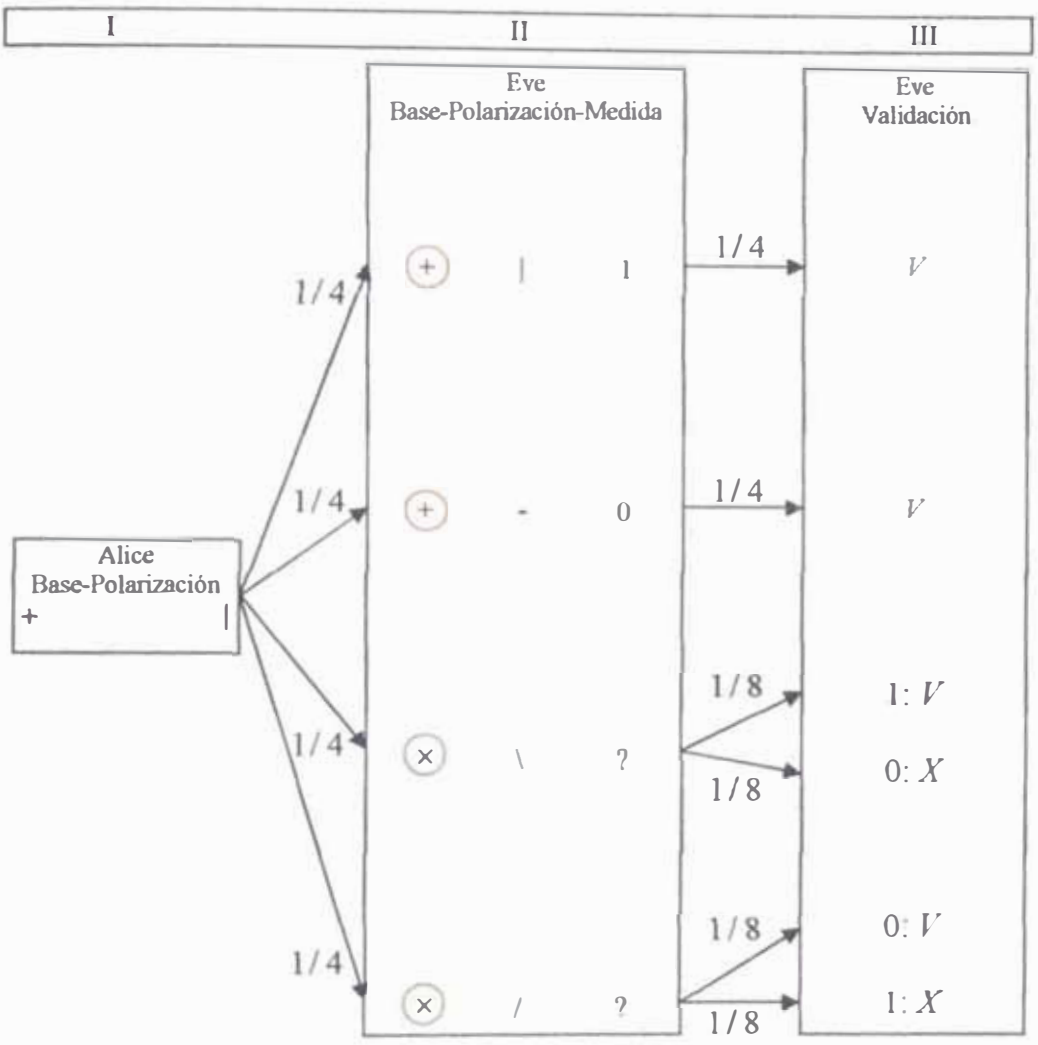


Figura 24: La máquina construida no tiene beamsplitters, el resultado que se obtiene es el mismo que la máquina convencional. El símbolo *V* significa que se obtuvo la polarización correcta y el símbolo *X* que se equivoco.

Paso I: Alice elije una de las dos bases, por ejemplo + y una de las dos polarizaciones posibles, por ejemplo |.

Paso II: Eve se decide por una de las bases y elije una polarización posible. Mide la señal. El 1 indica que si midió señal, el 0 que no midió señal y la ? indica que no se puede saber de antemano si medirá o no, todo depende del estado en que colapse el fotón.

Paso III: Eve trata de obtener información de las 4 posibilidades, pero sólo sabe que son absolutamente correctas (V) cuando su base es + es decir en 2 casos. Entonces Eve obtiene una coincidencia segura en 2/4 = 50% de la clave.

Pero hay 2 casos en los que Eve se equivoca de base entonces solo le queda adivinar el bit y acertará la mitad de las veces o sea 2/8.

En resumen, la clave de Eve comparado con Alice tiene las siguientes probabilidades de acertar y equivocarse:

$$p_{acertar}^{Eve} = \frac{2}{4} + \frac{2}{8} = \frac{3}{4} = 75\% \quad \cdots(57)$$

$$p_{equivocar}^{Eve} = \frac{2}{8} = \frac{1}{4} = 25\% \quad \cdots(58)$$

Exactamente igual a los resultados encontrados en la *máquina* convencional, ecuaciones 7 y 8.

4.3 Cálculo de probabilidades en un ataque parcial de probabilidad λ sin ruido

Si el espía ataca con una probabilidad λ entonces en la parte que no es atacada $(1-\lambda)$ Bob tendrá las siguientes probabilidades de acertar y equivocarse (ver ecuaciones 51 y 52):

$$p_{acertar}^{Bob} = (1-\lambda) \quad \cdots(59)$$

$$p_{equivocar}^{Bob} = 0 \quad \cdots(60)$$

Y en la parte λ atacada Bob tiene las siguientes probabilidades (ver ecuaciones 54 y 55):

$$p_{acertar}^{Bob} = \frac{3\lambda}{4} \quad \cdots(61)$$

$$p_{equivocar}^{Bob} = \frac{\lambda}{4} \quad \cdots(62)$$

En conclusión, de (59) y (61) la probabilidad total de Bob de acertar es:

$$p_{acertar}^{Bob} = (1-\lambda) + \frac{3}{4}\lambda = 1 - \frac{\lambda}{4} \quad \cdots(63)$$

Y de (60) y (62) probabilidad total de Bob de equivocarse es:

$$p_{equivocar}^{Bob} = \frac{\lambda}{4} \quad \cdots(64)$$

$$QBER = \frac{\lambda}{4} \quad \cdots(65)$$

Son iguales a las probabilidades de la máquina convencional (ecuaciones 13, 14 y 15).

¿Cuánto acierta Eve en este caso?

Eve ataca con una probabilidad λ es decir que en esta parte atacada tenemos (ver ecuaciones 57 y 58):

$$p_{acertar}^{Eve} = \frac{3\lambda}{4} \quad \cdots(66)$$

$$p_{equivocar}^{Eve} = \frac{\lambda}{4} \quad \cdots(67)$$

Y de los (1-λ) que no ataca sólo le queda adivinar acertando con probabilidad un 50%, es decir (1-λ)/2.

$$p_{acertar}^{Eve} = \frac{(1-\lambda)}{2} \quad \cdots(68)$$

$$p_{equivocar}^{Eve} = \frac{(1-\lambda)}{2} \quad \cdots(69)$$

En conclusión, de (66) y (68) Eve tiene en total la probabilidad de acertar:

$$p_{acertar}^{Eve} = \frac{3}{4}\lambda + \frac{(1-\lambda)}{2} = \frac{1}{2} + \frac{\lambda}{4} \quad \cdots(70)$$

Y de (67) y (69) tiene en total la probabilidad de equivocarse:

$$p_{equivocar}^{Eve} = \frac{\lambda}{4} + \frac{(1-\lambda)}{2} = \frac{1}{2} - \frac{\lambda}{4} \quad \cdots(71)$$

Son iguales a las probabilidades de la máquina convencional (ecuaciones 20 y 21).

4.4 Cálculo de probabilidades debido a un ruido δ% sin espía

En la Figura 25 se muestra visualmente el porcentaje de error que Bob obtiene en la parte de bits afectados por el ruido. Solo 1/3 cambiará a la polarización ortogonal y causará un error 1/6+1/6=1/3 los otros 2/3 cambiarán a polarizaciones en la otra base y causaran un error en 4 de las 8 posibilidades es decir 4/8 de 2/3, es decir 1/3, en total se tiene 1/3+1/3=2/3 de error, en conclusión, un ruido de δ% ocasiona en la clave de Bob un 2/3 δ% de error.

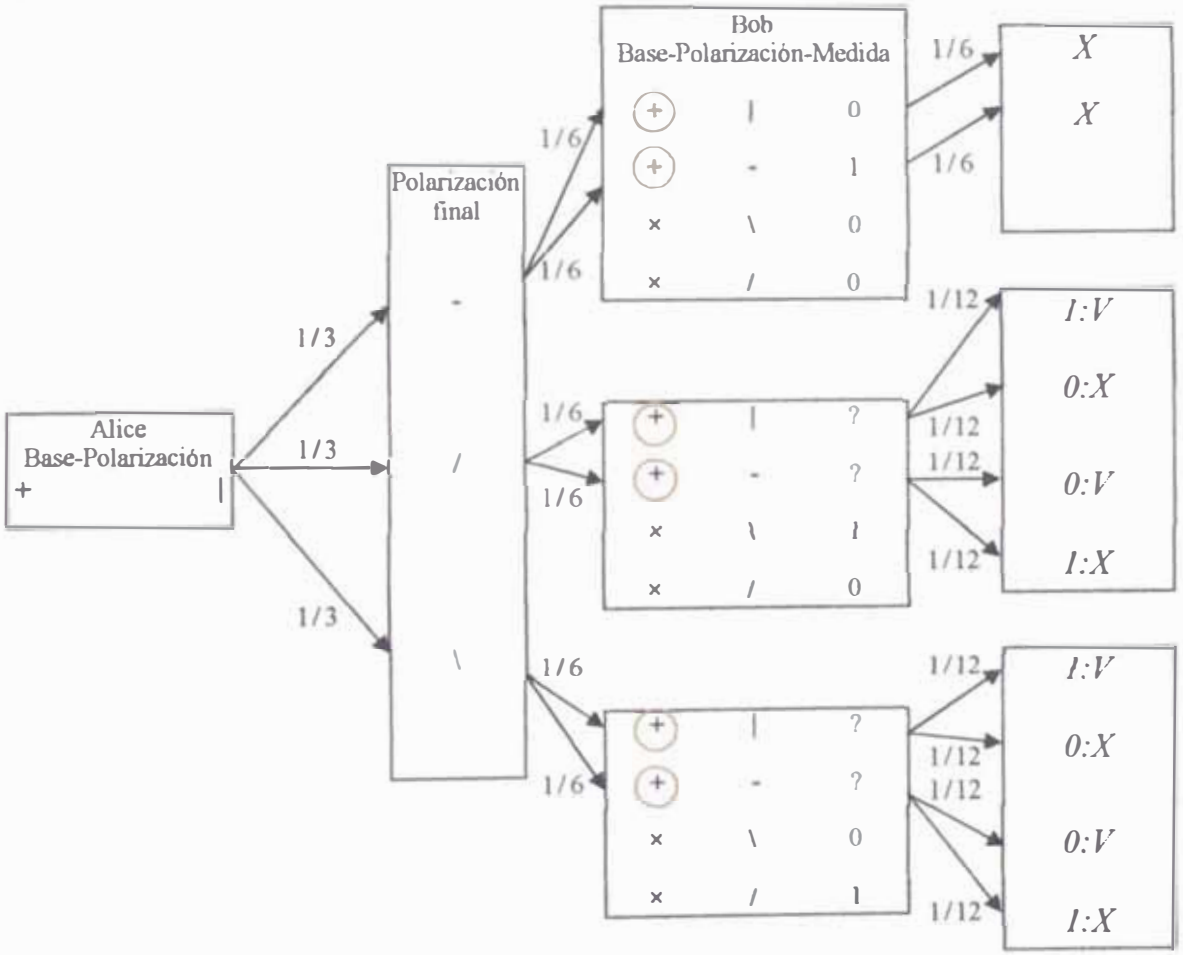


Figura 25: Un ruido de δ% en nuestra maquina ocasiona un error en la clave de Bob de 2/3 δ%. Igual al obtenido en la maquina convencional.

La Figura 25 muestra el análisis para el δ% de fotones afectados por el ruido, Bob obtiene las siguientes probabilidades de acierto y error:

$$p_{acertar}^{Bob} = \frac{4}{12}\delta\% = \frac{1}{3}\delta\% \quad \cdots(72)$$

$$p_{equivocar}^{Bob} = \frac{2}{6}\delta\% + \frac{4}{12}\delta\% = \frac{2}{3}\delta\% \quad \cdots(73)$$

Y del (100-δ)% que no es afectado por el ruido Bob tiene las siguientes probabilidades (ver ecuación 51 y 52):

$$p_{acertar}^{Bob} = (100-\delta)\% \quad \cdots(74)$$

$$p_{equivocar}^{Bob} = 0 \quad \cdots(75)$$

En conclusión, de (72) y (74) Bob tiene la probabilidad de acertar:

$$\boxed{p_{acertar}^{Bob} = \frac{1}{3}\delta\% + (100-\delta)\% = \left(100 - \frac{2}{3}\delta\right)\%} \quad \cdots(76)$$

Y de (73) y (75) Bob tiene la probabilidad de equivocarse:

$$\boxed{p_{equivocar}^{Bob} = \frac{2}{3}\delta\%} \quad \cdots(77)$$

$$\boxed{QBER = \frac{2}{3}\delta\%} \quad \cdots(78)$$

Son iguales a las probabilidades de la máquina convencional (ecuaciones 26, 27 y 28)

4.5 Cálculo de probabilidades debido a un ruido δ% con ataque parcial de probabilidad λ

Se tiene tres posibilidades de que el ruido afecte a la polarización del fotón:

1. **Ruido antes de que Eve mida**: En este caso Eve recibe un fotón con polarización cambiada, lo mide y tiene un 50% de cambiar su polarización, lo que significa modificar nuevamente la polarización del fotón, pero en resumen se puede decir que el fotón solo tuvo un cambio, desde su polarización inicial hasta la polarización obtenida por Eve. Luego Eve reenvía el fotón resultante con una polarización conocida por ella, lo que le da información al momento de construir su clave, pues conoce la polarización que recibe Bob.

2. **Ruido después de que Eva mida**: En este caso Eva recibe un fotón con polarización correcta, lo mide y tiene un 50% de cambiar su polarización, reenvía el fotón con una polarización conocida por ella, pero el ruido cambia esta polarización y pierde esta información reduciendo la probabilidad de acertar el bit, pues ahora no conoce la polarización que recibe Bob

3. **Ruido antes y después de que Eva mida**: En este caso Eve recibe un fotón con polarización cambiada, lo mide y tiene un 50% de cambiar su polarización, lo que significa modificar nuevamente la polarización del fotón, pero en resumen se puede decir que el fotón solo tuvo un cambio, desde su polarización inicial hasta la polarización obtenida por Eve. Luego Eve reenvía el fotón resultante con una polarización conocida por ella, pero el ruido cambia esta polarización y pierde esta información reduciendo la probabilidad de acertar el bit, pues ahora no conoce la polarización que recibe Bob.

De los tres casos, sólo en el primero Eve tiene información para poder aumentar su probabilidad de deducir la clave, conoce la polarización que recibe Bob, pero en los otros dos casos Eve pierde esta información pues el ruido cambia nuevamente la polarización.

Por tanto es en el primer caso donde Eve tiene más probabilidad de conocer la clave, por eso en esta tesis sólo se analiza este caso pues si el protocolo asegura que Eve no puede deducir la clave entonces se habrá comprobado que el protocolo es seguro.

De los bits que no son afectados por el ruido, (100-δ)%, es posible que sean intervenidos por Eve con una probabilidad λ entonces de las ecuación 61, Bob tiene la probabilidad de acertar:

$$p_{acertar}^{Bob} = \frac{3}{4}\lambda(100-\delta)\% = \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% \quad \cdots(79)$$

Y de la ecuación 62, Bob tiene la probabilidad de equivocarse:

$$p_{equivocar}^{Bob} = \frac{1}{4}\lambda(100-\delta)\% = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% \quad \cdots(80)$$

De los bits que no son afectados por el ruido (100-δ)% se tiene una probabilidad de (1-λ) que no sean interceptados por el espía entonces de la ecuación 51, Bob acierta:

$$p_{acertar}^{Bob} = (1-\lambda)(100-\delta)\% = (100-\delta-100\lambda+\lambda\delta)\% \quad \cdots(81)$$

Y de la ecuación 52, Bob se equivoca con una probabilidad:

$$\boxed{p_{equivocar}^{Bob} = 0} \quad \cdots(82)$$

De los bits que son afectados por el ruido, δ%, estos son intervenidos por Eve con una probabilidad λ y es posible que algunos regresen a su polarización original. En la Figura 26 se muestra el análisis.

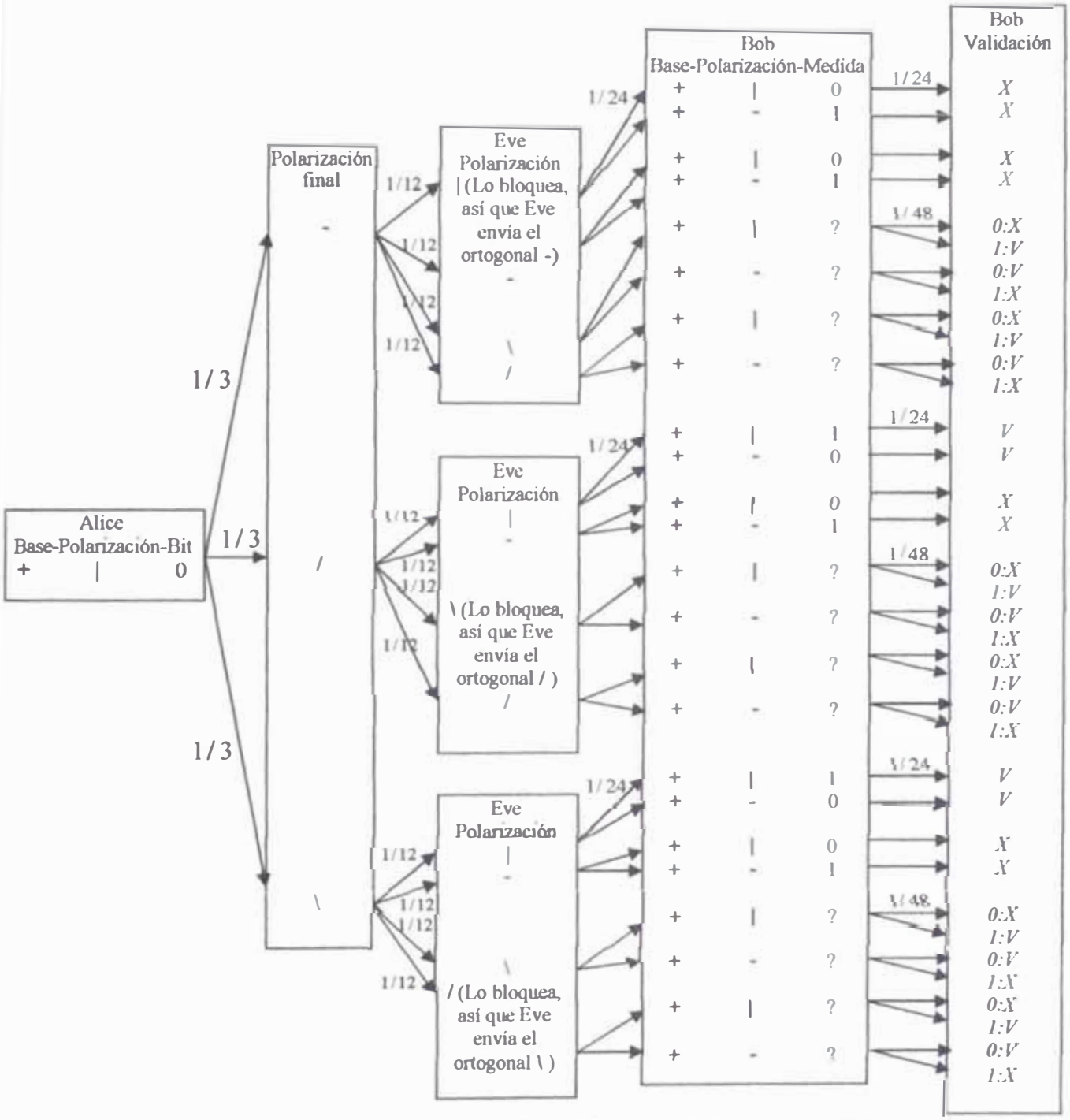


Figura 26: El espía interviene con una probabilidad λ. La parte de la clave de Bob afectada por el ruido δ% tiene un error de 7δ/12 %.

De la Figura 26, tenemos que Bob acierta:

$$p_{acertar}^{Bob} = \left(\frac{4}{24} + \frac{12}{48}\right)\lambda\delta\% = \frac{5}{12}\lambda\delta\% \quad \cdots(83)$$

Y se equivoca:

$$p_{equivocar}^{Bob} = \left(\frac{8}{24} + \frac{12}{48}\right)\lambda\delta\% = \frac{7}{12}\lambda\delta\% \quad \cdots(84)$$

Pero además, el (1-λ) del δ% que no es intervenido por Eve, solo es afectado por el ruido y se tendrá un acierto de 1/3 y un error del 2/3 (ver ecuaciones 72 y 73).

$$p_{acertar}^{Bob} = \frac{1}{3}(1-\lambda)\delta\% = \left(\frac{1}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(85)$$

$$p_{equivocar}^{Bob} = \frac{2}{3}(1-\lambda)\delta\% = \left(\frac{2}{3}\delta - \frac{2}{3}\lambda\delta\right)\% \quad \cdots(86)$$

En conclusión, de (79), (81), (83) y (85), Bob acierta con probabilidad:

$$\begin{aligned} p_{acertar}^{Bob} &= \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% + (100 - \delta - 100\lambda + \lambda\delta)\% + \frac{5}{12}\lambda\delta\% + \left(\frac{1}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \\ &= \left(100 - \frac{2}{3}\delta - 25\lambda + \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(87)$$

Y de (80), (82), (84) y (86), Bob se equivoca con probabilidad:

$$p_{equivocar}^{Bob} = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% + 0 + \frac{7}{12}\lambda\delta\% + \left(\frac{2}{3}\delta - \frac{2}{3}\lambda\delta\right)\% = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(88)$$

$$QBER = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\% \quad \cdots(89)$$

Son iguales a las probabilidades de la máquina convencional (ecuaciones 37, 38 y 39)

¿Cuánto acierta Eve en este caso?

De los bits no afectados por el ruido (100-δ)%, es probable que sean atacados con una probabilidad λ entonces de la ecuación 66, Eve acierta:

$$p_{acierta}^{Eve} = \frac{3}{4}\lambda(100-\delta)\% = \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% \quad \cdots(90)$$

Y de la ecuación 67, Eve se equivoca:

$$p_{equivoca}^{Eve} = \frac{1}{4}\lambda(100-\delta)\% = \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% \quad \cdots(91)$$

De los bits no afectados por el ruido (100-δ)%, es probable que el (1-λ) no sean atacados entonces a Eve sólo le queda adivinar y acierta los bits con una probabilidad del 50%:

$$p_{acierta}^{Eve} = \frac{1}{2}(1-\lambda)(100-\delta)\% = \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% \quad \cdots(92)$$

$$p_{equivoca}^{Eve} = \frac{1}{2}(1-\lambda)(100-\delta)\% = \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% \quad \cdots(93)$$

De los bits que son afectados por el ruido δ%, existe la probabilidad λ de ser espiados, el análisis se muestra en la Figura 27.

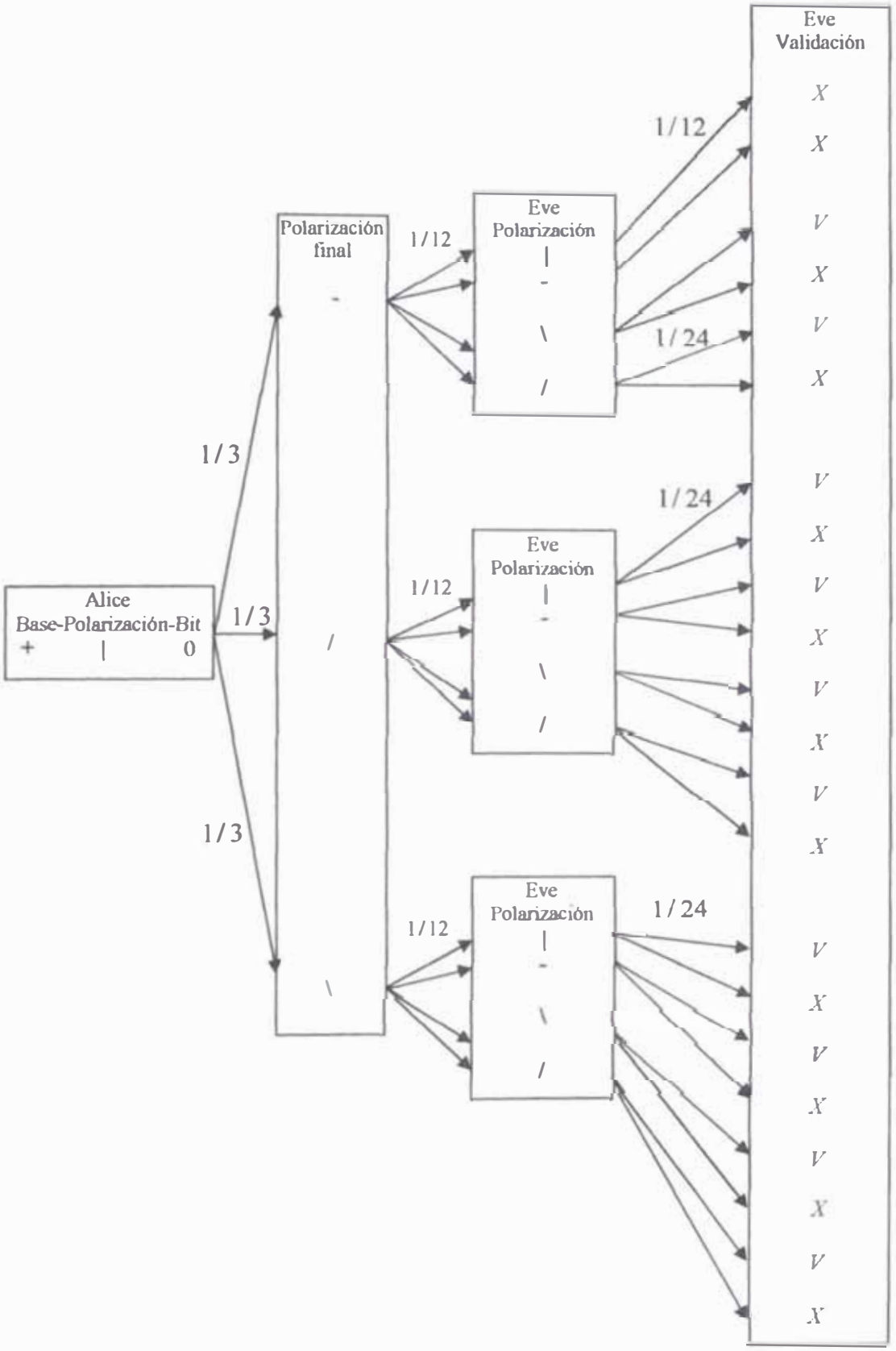


Figura 27: El espía interviene con una probabilidad ½. La parte de la clave de Eve afectada por el ruido ó% tiene un acierto de 5½ó/12 %.

En la Figura 27 se observa que en un solo caso se puede asegurar con certeza que Eve se equivocará, los otros casos son inciertos y tiene un 50% de acertar o equivocarse, por tanto se obtiene:

$$p_{acertar}^{Eve} = \left(\frac{10}{24}\right)\lambda\delta\% = \frac{5}{12}\lambda\delta\% \quad \cdots(94)$$

$$p_{equivocar}^{Eve} = \left(\frac{2}{12}\lambda\delta + \frac{10}{24}\lambda\delta\right)\% = \frac{7}{12}\lambda\delta\% \quad \cdots(95)$$

De los bits que son afectados por el ruido δ%, existe la probabilidad (1-λ)δ% que no sean espiados, entonces a Eve sólo le queda adivinar y acierta los bits con una probabilidad del 50%:

$$p_{acertar}^{Eve} = \frac{1}{2}(1-\lambda)\delta\% = \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \quad \cdots(96)$$

$$p_{equivocar}^{Eve} = \frac{1}{2}(1-\lambda)\delta\% = \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \quad \cdots(97)$$

En conclusión, de (90), (92), (94) y (96) Eve tiene una probabilidad de acertar:

$$\begin{aligned} p_{acertar}^{Eve} &= \left(75\lambda - \frac{3}{4}\lambda\delta\right)\% + \left(50 - \frac{\delta}{2} - 50\lambda + \frac{\lambda\delta}{2}\right)\% + \frac{5}{12}\lambda\delta\% + \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \\ &= \left(50 + 25\lambda - \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(98)$$

Y de (91), (93), (95) y (97) Eve tiene una probabilidad de equivocarse:

$$\begin{aligned} p_{equivocar}^{Eve} &= \left(25\lambda - \frac{1}{4}\lambda\delta\right)\% + \left(50 - \frac{1}{2}\delta - 50\lambda + \frac{1}{2}\lambda\delta\right)\% + \frac{7}{12}\lambda\delta\% + \left(\frac{1}{2}\delta - \frac{1}{2}\lambda\delta\right)\% \\ &= \left(50 - 25\lambda + \frac{1}{3}\lambda\delta\right)\% \end{aligned} \quad \cdots(99)$$

Son iguales a las probabilidades de la máquina convencional (ecuaciones 48 y 49)

4.6 Resumen del cálculo probabilístico

1. Se han deducido las fórmulas probabilísticas que gobiernan la transmisión de qubits en la máquina construida (párrafo 2.3.1.2). Estas fórmulas resultan ser iguales a los que se dedujo anteriormente para máquinas ideales. Las ecuaciones 87, 88, 89, 98 y 99 (Párrafo 4.5) son iguales a las ecuaciones I, II, III, IV y V (párrafo 2.3.1.3) respectivamente. Lo que demuestra que ambas máquinas en principio son equivalentes

2. Las formulas probabilísticas deducidas toman en cuenta tanto el ruido en la transmisión como el ataque de espias, por tanto son ecuaciones completas que describen cualquier caso de transmisión que utilice el protocolo cuántico BB84. Estas fórmulas generales ni las propias deducciones se encuentran publicadas en ningún artículo conocido, lo que es un aporte propio de esta tesis.

3. Estas fórmulas permitirán comprobar el buen funcionamiento de cualquier máquina de criptografía cuántica construida que utilice en protocolo BB84.

Capítulo 5

Simulación computarizada de la transmisión de una clave cuántica

Como se menciono en el Capítulo 4, la máquina convencional tiene un sistema de medida de Bob formado por un beamsplitter no polarizador, dos beamsplitters polarizadores, una lámina retardadora media onda y cuatro detectores fotodiodos de avalancha. En cambio nuestra máquina reemplaza todo esto por un disco giratorio con cuatro polarizadores y un fototransistor. Esta simplificación es simulada en el programa para obtener resultados que se obtendrían en nuestra máquina. Además en la máquina convencional Alice utiliza una fuente de fotones individuales y nuestra máquina utiliza pulsos de fotones, sin embargo en la simulación se puede programar fotones individuales.

Los programas de simulación se han escrito en Visual C# y permite simular el envío de hasta 100 mil fotones. El programa también simula ruido en la transmisión, logrando corregir con éxito la clave siempre y cuando el QBER sea menor o igual que 20% y con una buena probabilidad de éxito si el QBER está entre 20% y 25%. El programa de simulación sacrifica el 50% de la clave para calcular el QBER, de esta manera la mitad de la clave se hace pública y ya no sirve, pero aún queda la otra mitad que solo es conocida por Alice y Bob.

El programa muestra que es imposible que un espía obtenga la clave mediante el uso de métodos de ataque conocidos

- Man in the Middle: El espía Eve se coloca entre Alice y Bob e intercepta todos los fotones enviados por Alice, intenta medir su polarización y reenvía el resultado a Bob.
- Photon Number Splitting: El espía Eve desvía aleatoriamente algunos fotones enviados por Alice usando beamsplitters, intenta medir su polarización y reenvía el resultado a Bob.

Se puede idear variaciones de estos métodos pero todos modificaran con alguna probabilidad las claves obtenidas por Alice y Bob, es por eso que si el QBER es mayor

que cierto valor, se descarta la clave y se empieza de nuevo. En (27) Peter Shor y John Preskill muestran que sin espías se puede esperar un QBER <11%.

En la Figura 28 se muestra el diagrama de bloques del programa. Usualmente se recomienda aceptar un error máximo antes de la corrección ($E_{máximo}$) menor que 11% y un error aceptable en la transmisión ($E_{límite}$) menor que 1%, estos parámetros no son constantes en el programa y el usuario puede usar el que desee con el riesgo que supone la seguridad. Transmitir con un QBER diferente de cero significa que algunos caracteres del mensaje desencriptado por Bob podrían ser erróneos.

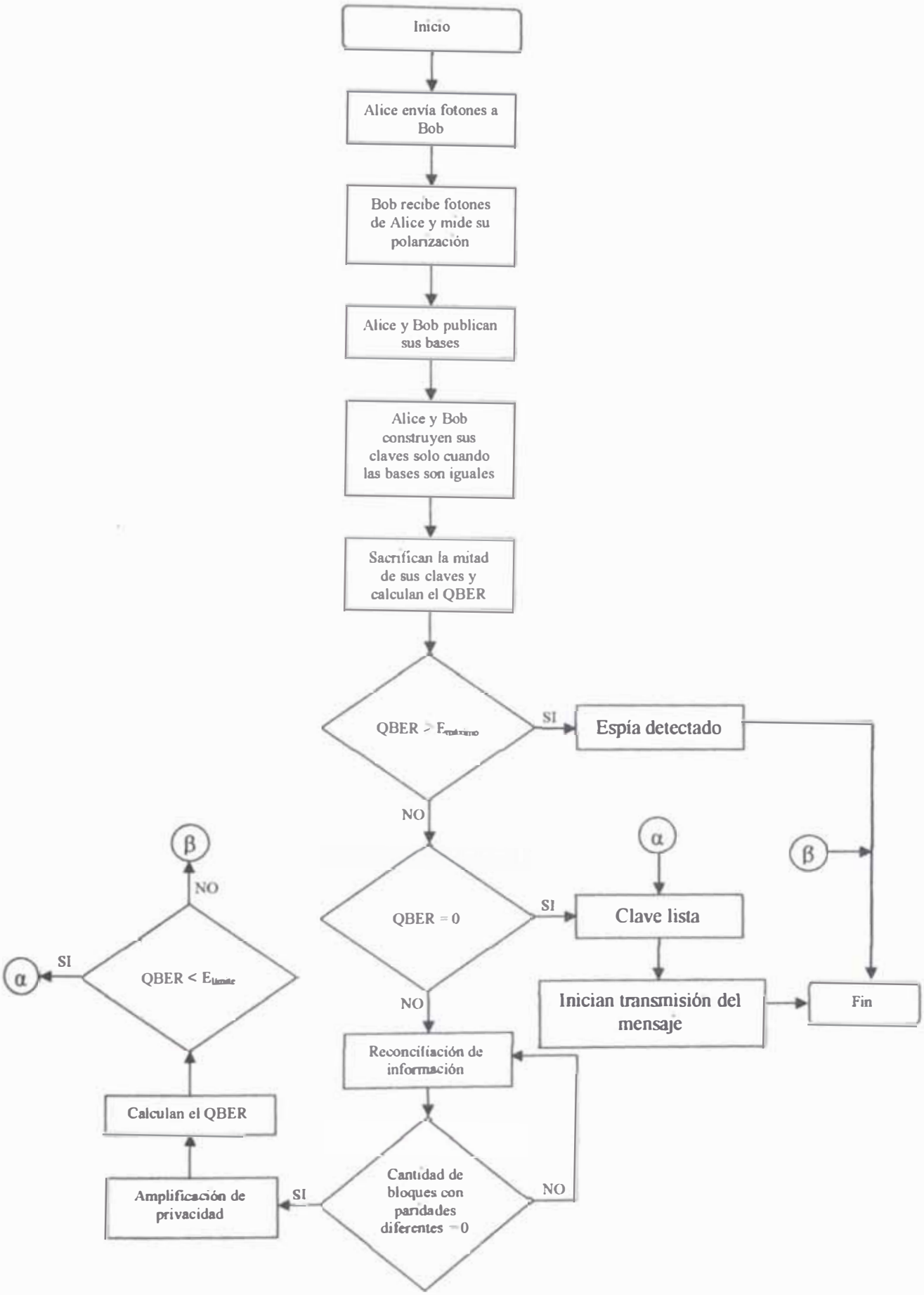


Figura 28: Diagrama de análisis de Alice y Bob en el programa.

5.1 Ejemplo de transmisión con ruido y sin espía

En el diseño original, la máquina cuenta con un sistema de beamsplitters que permite obtener la polarización del fotón siempre y cuando se mida con la misma base. En el apéndice C se explica detalladamente este sistema de beamsplitters.

En la máquina construida por falta de recursos económicos no se logro adquirir beamsplitters y en su lugar se utilizó discos polarizadores para la medida de Bob, es decir que nuestra máquina no mide a nivel de bases como el protocolo original, sino a nivel de polarizaciones con lo que puede ocurrir que en algunos casos se bloquee la polarización enviada por Alice, es en este caso donde el software hace una corrección siguiendo la regla "***Si bloqueo la polarización entonces la polarización enviada por Alice es la ortogonal***" con esto se salva la situación de no tener beamsplitters.

A continuación se muestra un ejemplo de cómo funciona el programa con un ruido del 10% y sin espías:

1. Alice desea enviar un mensaje de una letra, por ejemplo la letra **z**, cuyo código ASCII es 122, en binario es 1111010, es decir que n=**8** bits.

2. Se elige arbitrariamente[50] un δ igual a $2n$, entonces se genera una cadena aleatoria a de $4n+\delta=6n=48$ bits y otra cadena aleatoria b para la base, con la que se selecciona las polarizaciones correspondientes y se almacena en la cadena c, por ejemplo:

3. Alice envía las polarizaciones a Bob (fila c de la tabla anterior), pero como hay un ruido del 10%, entonces de las 48 polarizaciones, 5 polarizaciones llegan modificadas a Bob (cuadros amarillos).

4. Bob recibe los 48 bits (polarizaciones) y mide según una cadena aleatoria de bases b' y una cadena de polarizaciones c', decodificando en una cadena a'.

[50] La elección de δ depende de cuánto ruido esperamos en la transmisión, eso depende de la calidad de los equipos y de las condiciones atmosféricas. El δ se determina experimentalmente.

5. Alice y Bob solo tomarán en cuenta aquellos bits cuyas bases coincidan, fondo verde, se espera tener una clave de 24 bits, en este ejemplo se obtuvo 25:

   Alice:

   Las polarizaciones que fueron afectadas por el ruido generan un bit erróneo en la clave de Bob.

6. Ambos forman así sus claves, Alice selecciona aleatoriamente la mitad, en este caso 12, y comunica a Bob las posiciones para comparar (fondo celeste). Se observa que Bob tiene 2 bits erróneos.

Alice	1	0	0	0	1	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1
Bob	1	0	0	1	1	1	0	0	1	1	0	1	0	1	0	0	1	0	0	1	0	1	1	0	1

7. Comparan para hallar el QBER en este ejemplo se tiene 12 bits sacrificados (fondo celeste) de los cuales 1 es erróneo entonces se obtiene un QBER=1/12=8.3%.

Alice	0	1	0	0	1	0	0	0	1	1	1	1
Bob	0	1	0	1	1	0	0	0	1	1	1	1

8. Como se comento al principio de este Capítulo, un QBER<11% es aceptable, así que se procede a la corrección de errores tal como se explico anteriormente, se divide la clave que queda en bloques de 4 y se compara su paridad. Si son diferentes se elimina todo el bloque, pero si son iguales solo se elimina el último bit y el resto queda en la clave.

Alice	1	0	0	1	0	1	0	1	0	1	0	0	0
Bob	1	0	1	1	0	1	0	1	0	1	0	0	0

En este ejemplo por comodidad se utilizó un $\delta=2n$ para tener pocos bits, así que se realizará una sola ronda de corrección de errores.

El bloque amarillo de Alice tiene paridad par y el de Bob paridad impar así que se eliminan, en el bloque verde ambos tienen paridad par y en el bloque azul ambos tienen paridad impar, así que se procede a eliminar sus correspondientes últimos bits, quedando las claves para Alice y Bob de la siguiente manera:

Alice	0	1	0	0	1	0	0
Bob	0	1	0	0	1	0	0

Se obtiene una clave de 7 bits, pero se necesita 8 bits para transmitir un carácter, usualmente se elije un δ grande para no tener este problema de una clave muy pequeña. Alice y Bob deben ponerse de acuerdo en una técnica para completar las claves, en esta tesis se completa lo que falta con los primeros bits, aunque podría también elegirse una selección aleatoria.

Se obtiene por tanto:

Alice	0	1	0	0	1	0	0	0
Bob	0	1	0	0	1	0	0	0

9. Luego se amplifica la privacidad, el objetivo es reducir la información que tiene un posible espía aumentando los errores en su clave, esto se logra mezclando los bits usando alguna función. En esta tesis se selecciona aleatoriamente dos bits y se realiza la operación XOR para luego reemplazar el resultado en cualquier posición aleatoria una cantidad de veces igual a la longitud de la clave.

   La clave tiene 8 bits, así que repetiremos la operación 8 veces, los bits elegidos tendrán fondo amarillo y el que se reemplazará color verde.

Primera mezcla:

Alice	0	1	0	0	1	0	0	0
Bob	0	1	0	0	1	0	0	0

Resulta:

Alice	0	1	0	1	1	0	0	0
Bob	0	1	0	1	1	0	0	0

Segunda mezcla:

Alice	0	1	0	1	1	0	0	0
Bob	0	1	0	1	1	0	0	0

Resulta:

Alice	0	1	0	1	0	0	0	0
Bob	0	1	0	1	0	0	0	0

A medida que se avanza la clave se va transformando, el éxito de la amplificación se basa en que si un espía empieza a mezclar sus bits, en algún momento mezclará un bit correcto con uno incorrecto obteniendo un resultado que no coincide con el bit de Alice y Bob, aumentando así la cantidad de bits erróneos de su clave. Luego de 8 amplificaciones se podría obtener, por ejemplo:

Alice	1	1	0	1	0	0	1	0
Bob	1	1	0	1	0	0	1	0

10. Finalmente Alice y Bob tienen sus claves idénticas y están listos para transmitir el mensaje.

5.2 Simulación de transmisión sin espía y sin ruido

Idealmente la transmisión se realiza sin ruido y sin ningún espía que potencialmente modifique la polarización original. Como se demuestra en la práctica esto no es lo común, por ejemplo, pruebas realizadas con la máquina construida por Henning Weir, en su Tesis de Diplomado en Física (32), obtiene un QBER entre 2.8% y 5.0% (36). Chris Erven en su Tesis de Maestría en Física (30) obtiene un QBER promedio de 9.3%. Tobias Schmitt-Manderbach en su Tesis de Doctor en Física (31) obtiene un QBER entre 2.86% y 5.85% y Martin Hendrych en su Tesis de Doctor en Física (33) utiliza fibra óptica y obtiene un QBER promedio de 0.32%. Nuestra máquina a diferencia de las construidas en otras tesis no envía fotones individuales, en su lugar envía pulsos de fotones, es por eso que se obtiene un QBER del 0% pero esto no es una buena noticia pues al enviar un pulso de fotones, también se está expuesto a que espías usando el método PNS logren obtener la clave sin dificultad y experimentalmente se confirma este temor, de allí la necesidad que en un proyecto futuro se construya una fuente de fotones individuales, ya se tiene los conocimientos necesarios y suficientes para construir tal fuente de fotones individuales, solo falta una financiación apropiada para adquirir las partes ópticas.

Se ejecuta el programa BB84 exe y aparece el formulario principal (Figura 29).

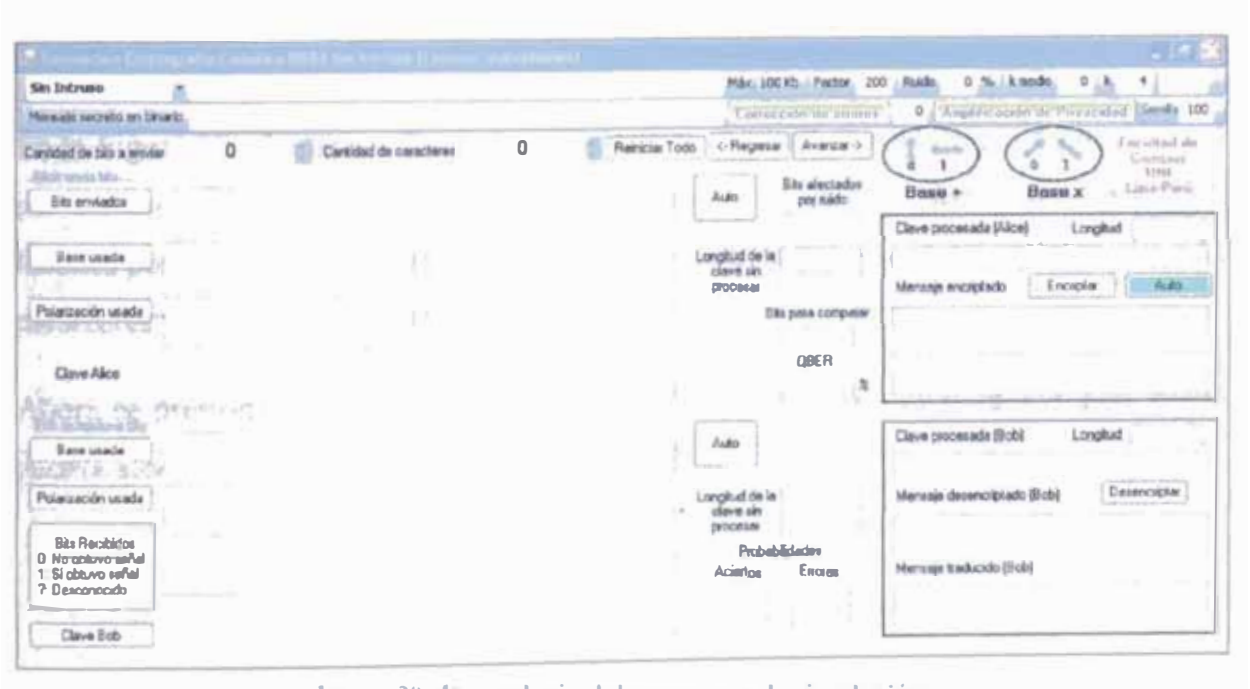


Figura 29: Formulario del programa de simulación.

Se escribe el mensaje que se desea enviar, para que el programa calcule la cantidad de bits necesarios para crear la clave (Figura 30)

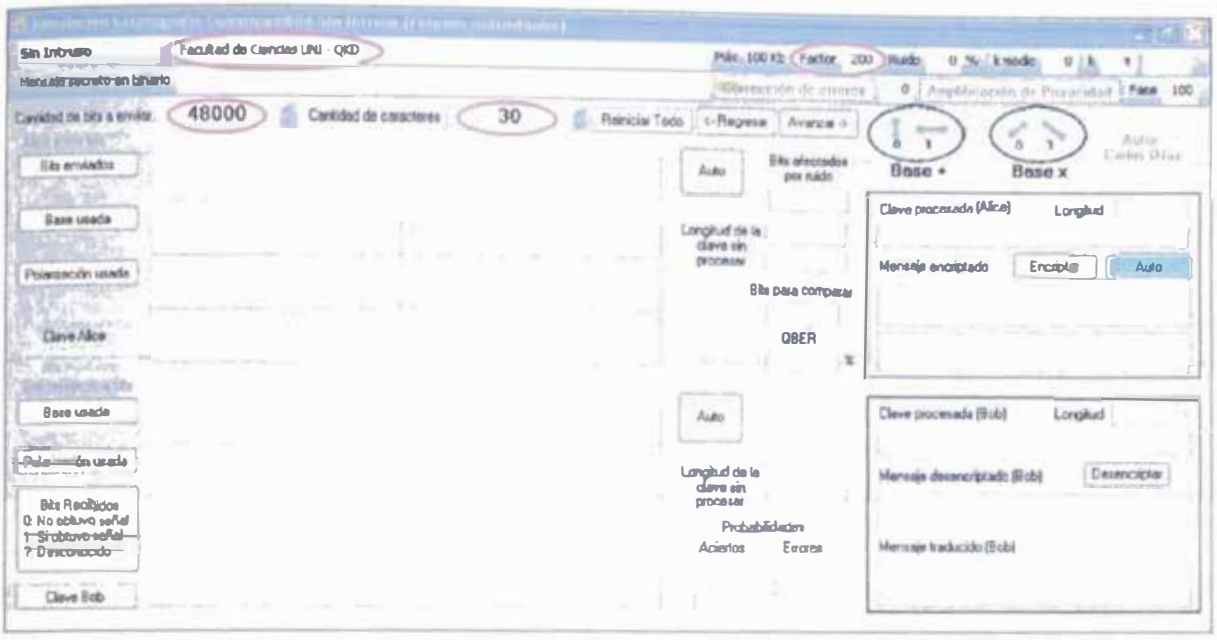


Figura 30: Se escribe el mensaje secreto que se desea enviar.

Cada carácter se representa por su código ASCII en binario, es decir por 8 bits, como el protocolo BB84 genera una clave con aproximadamente el 50% de los bits enviados por Alice, entonces se necesita como mínimo 16 bits por carácter.

Sin embargo debido al sacrificio de bits para calcular el QBER y a la posterior eliminación de bits durante la corrección de errores se tiene que utilizar más bits por carácter.

En la Figura 30, el cuadro "Factor" del formulario muestra cuantas veces 8 bits se usará por carácter. En este programa se uso un factor de 200, es decir que se empleará 1600 fotones por carácter. El mensaje secreto es "Facultad de Ciencias UNI - QKD", tiene 30 caracteres y Alice enviará 48 mil fotones.

Ahora se presiona el botón "Bits enviados" del panel de Alice (Figura 31). Este botón genera aleatoriamente los bits que se enviará a Bob

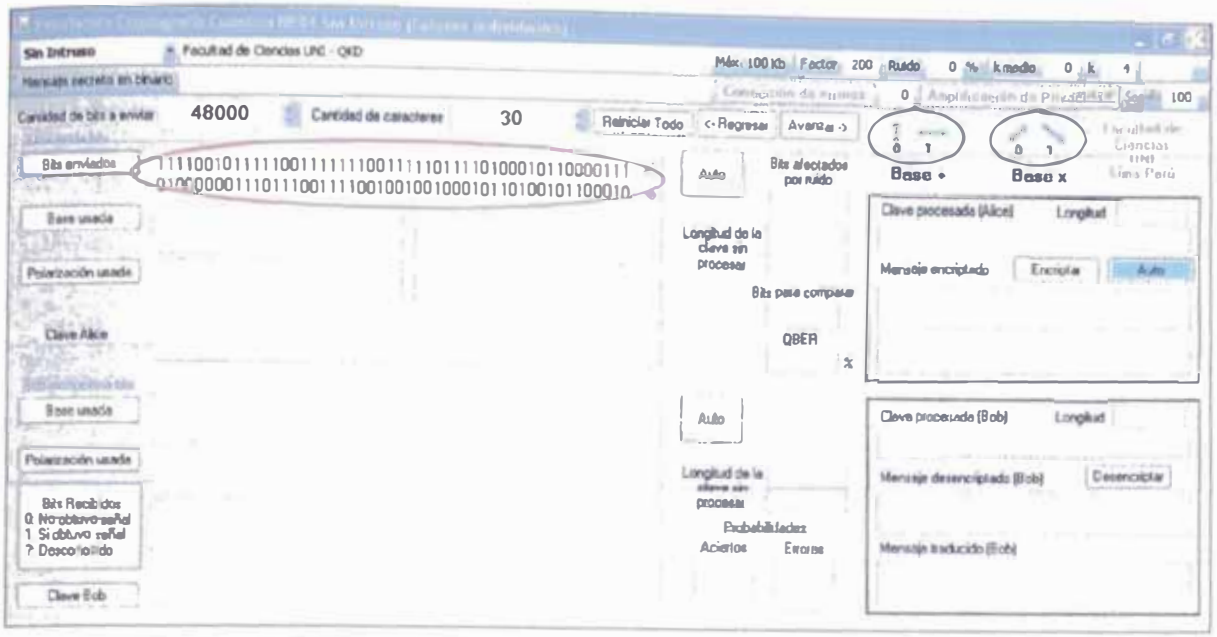


Figura 31: Bits elegidos aleatoriamente por Alice.

Cada bit que se enviará será por medio de la base + ó ×, se presiona el botón "Base usada" para que el programa seleccione aleatoriamente las bases de envío (Figura 32).

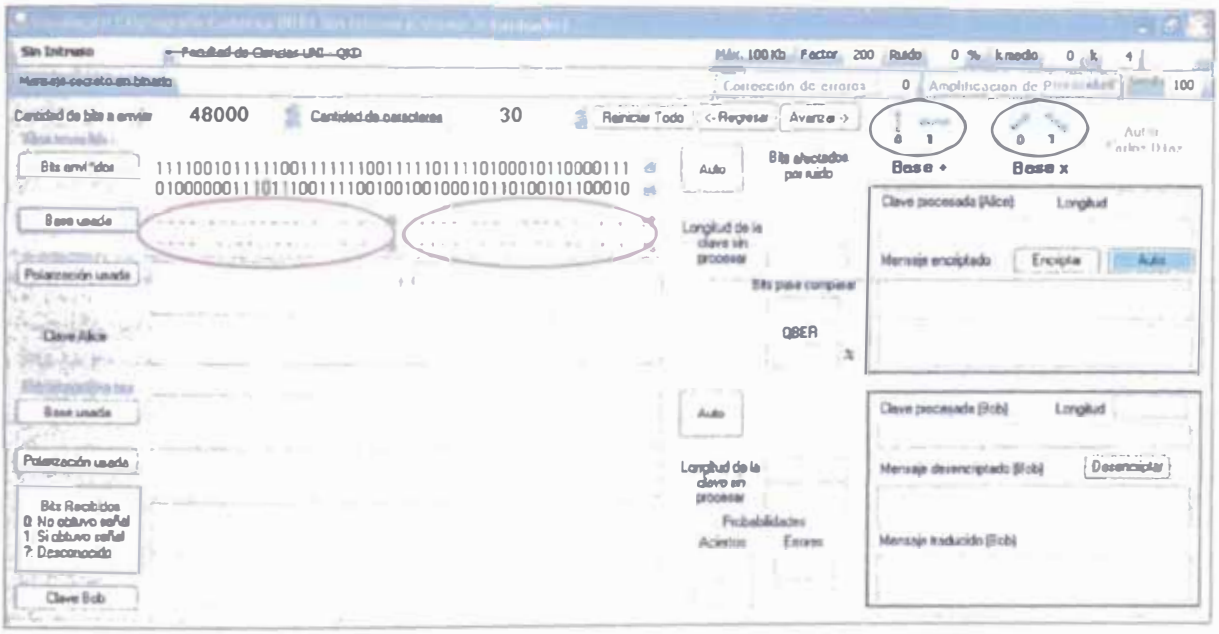


Figura 32: Bases elegidas aleatoriamente por Alice.

El primer cuadro de la Figura 32 muestra las bases elegidas por Alice para enviar los bits y el segundo cuadro muestra las bases con que realmente llegan los fotones a Bob y que debido al ruido algunas pueden ser distintas a las elegidas, en este ejemplo no hay ruido entonces ambos cuadros son iguales.

En este punto el programa sabe que bit enviará y que base usará, ahora debe elegir la polarización de cada fotón de acuerdo a la base y al bit, clic al botón "Polarización usada" (Figura 33).

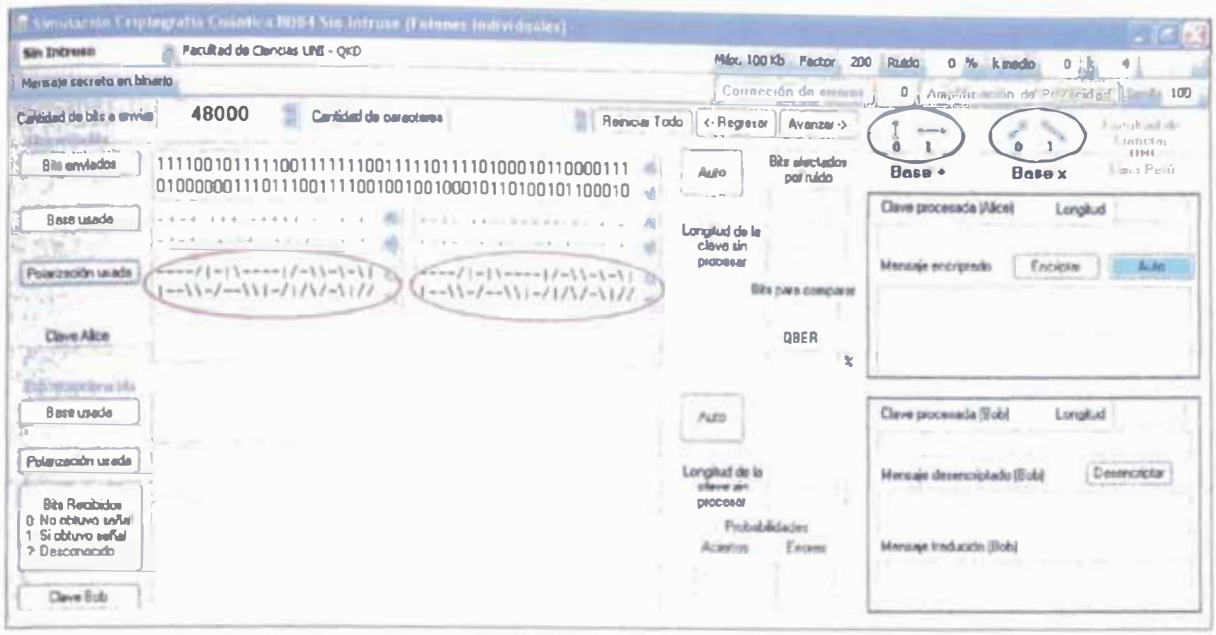


Figura 33: Polarizaciones elegidas aleatoriamente por Alice.

Igual que en el caso de las bases, los dos cuadros son iguales si es que no hay ruido. Si hubiese ruido, algunas polarizaciones que viajan hacia Bob serian distintas.

Una vez que Alice ya tiene lista toda la información (polarización) acerca de los bits que enviará, avisa a Bob (por cualquier medio) que iniciará el envió y este elige una base aleatoria para recibir los bits de Alice, presionamos el botón "Base usada" del panel de Bob (Figura 34).

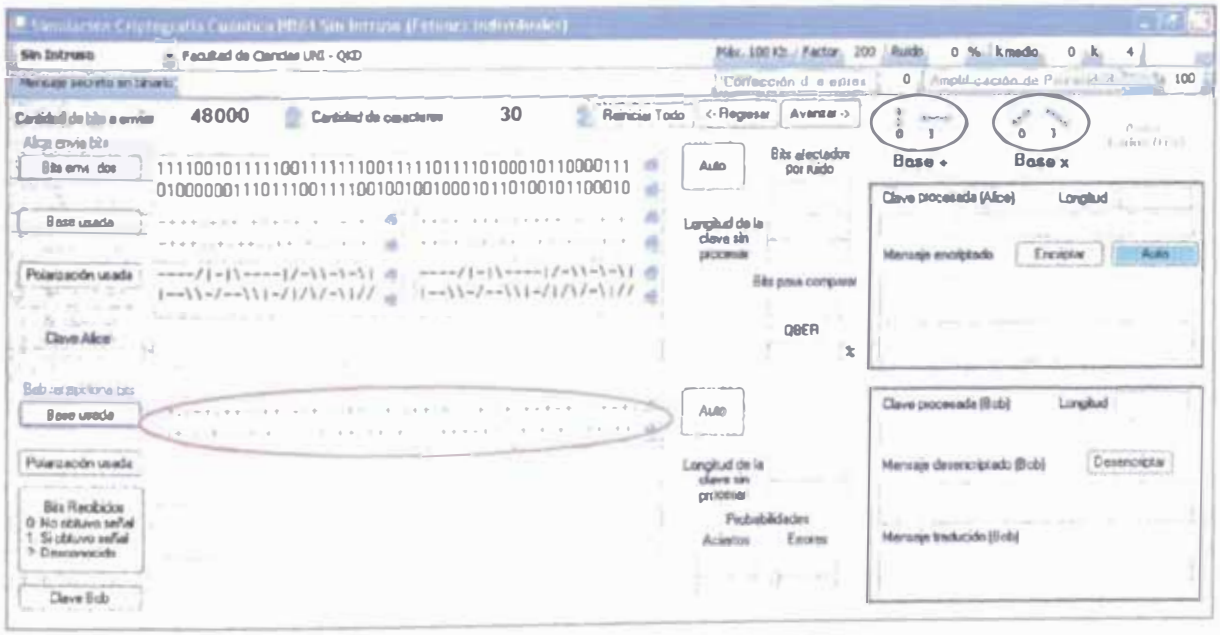


Figura 34: Bases que Bob usará para recibir los fotones de Alice.

A continuación Bob selecciona aleatoriamente las polarizaciones correspondientes a la base elegida y así medir la polarización del fotón enviado por Alice, clic al botón "Polarización usada" (Figura 35).

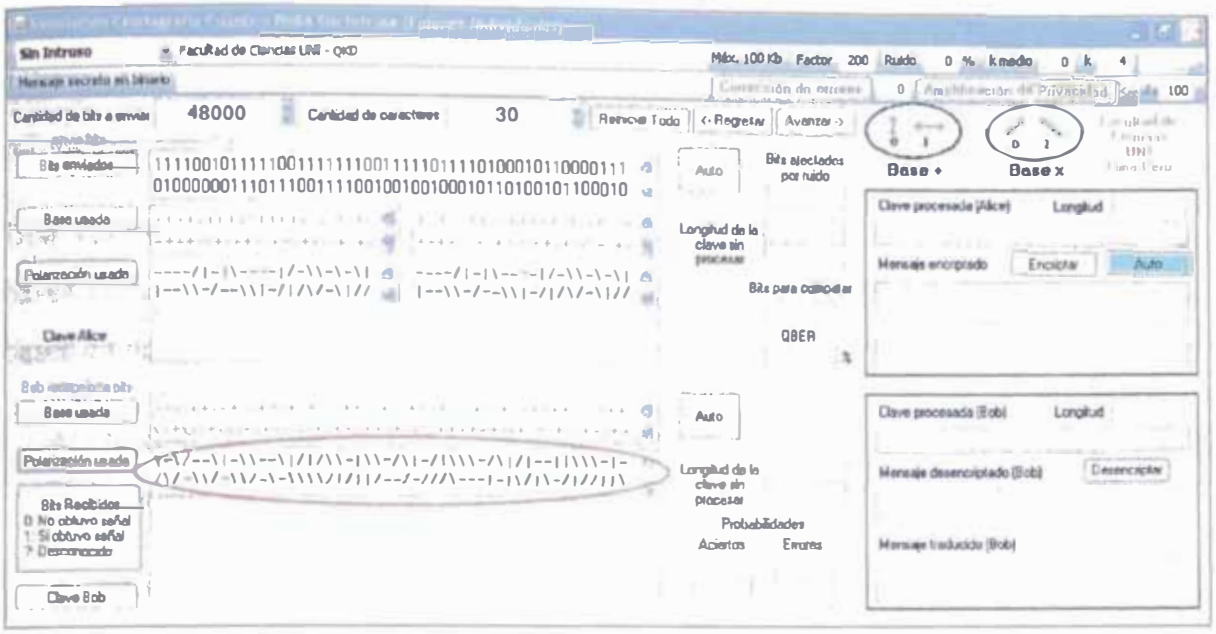


Figura 35: Polarizaciones usadas por Bob.

Una vez que las elecciones por ambos bandos están decididas, se inicia la transmisión vía un canal cuántico, simulado por el programa, donde Bob mide la polarización de cada fotón enviado por Alice (Figura 36).

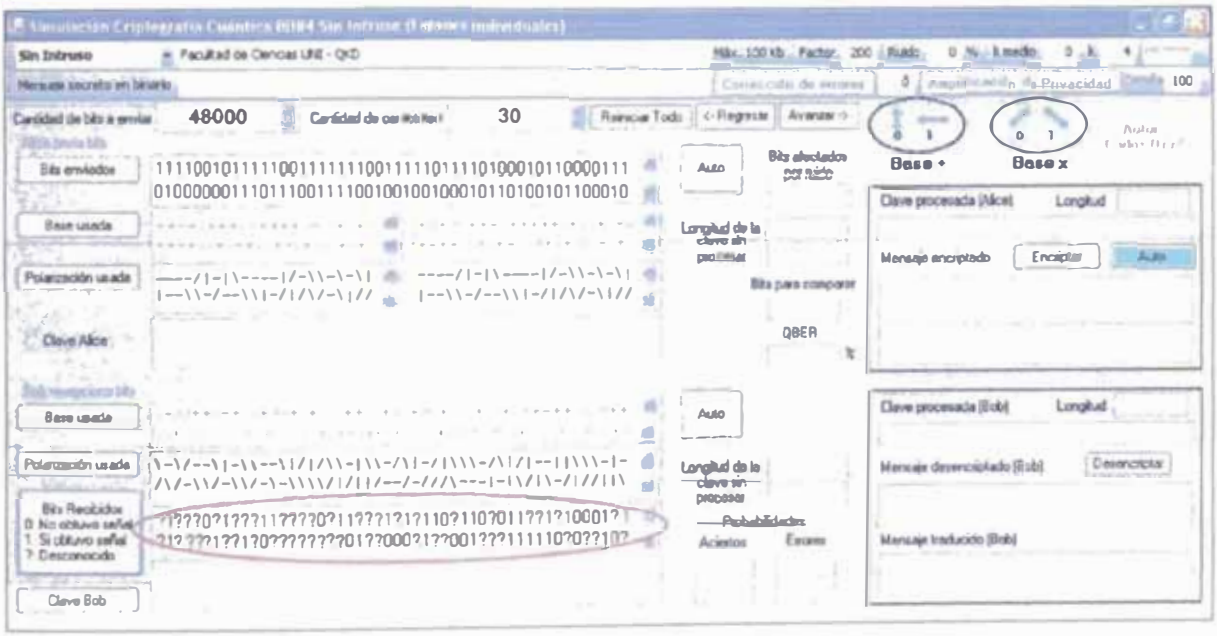


Figura 36: Medidas obtenidas por Bob.

Como las bases son conjugadas entonces si Bob utiliza la misma base que Alice podría medir la llegada del fotón en su detector si es que su polarización de medida coincide con la polarización del fotón, lo que en la Figura 36 se representa por "1", pero si Bob utiliza una polarización ortogonal a la del fotón entonces su detector no lo medirá, lo que en la Figura 36 se representa por "0", en cualquier caso Alice podrá deducir el bit enviado por Alice. Otro situación es cuando Bob usa la base conjugada a la de Alice,

entonces el fotón colapsará en cualquiera de las polarizaciones de la base conjugada y Bob podría detectar o no la llegada del fotón, en la Figura 36 esta situación se representa por "?".

Una vez realizadas las medidas, el protocolo indica que Alice y Bob publiquen sus bases vía un canal clásico, simulado por el programa, y que tomen en cuenta solo las bases en las que coincidieron, de tal forma que:

- Si Bob tuvo una medida ("1") entonces su polarización coincidió con la de Alice y puede saber el bit que le envió Alice.
- Si Bob no midió ("0") entonces su polarización fue ortogonal a la de Alice y entonces toma la polarización ortogonal a la que él uso para saber el bit de Alice.

Para mostrar las claves de Bob y Alice se presiona el botón "Clave Bob". En la Figura 37 se muestra el resultado.

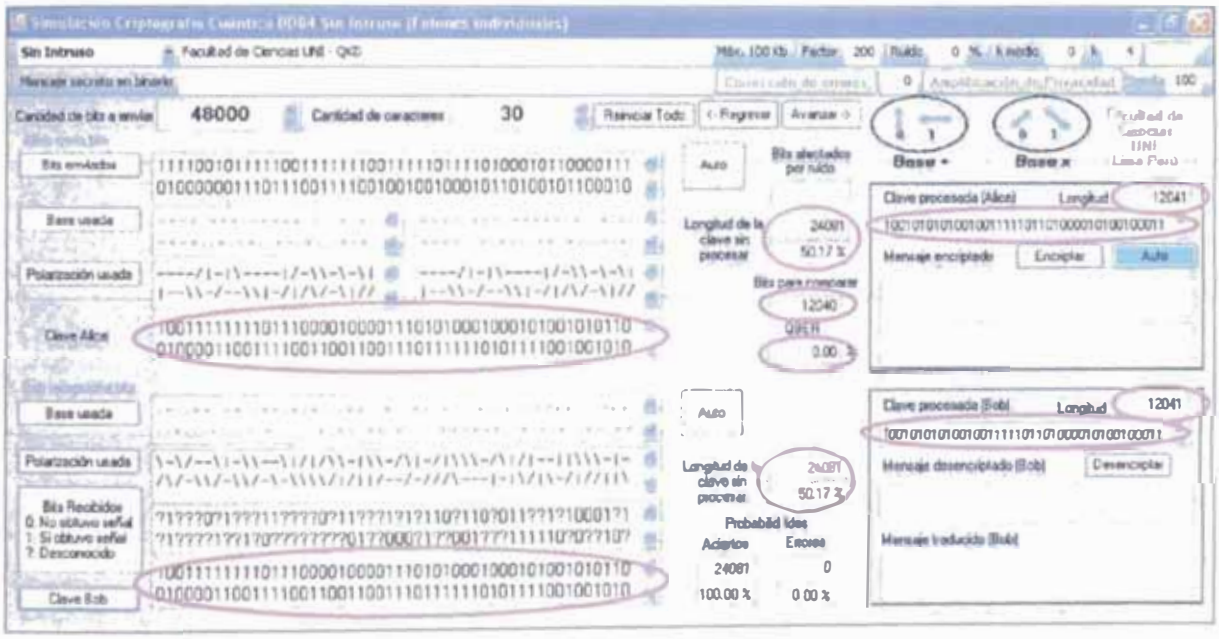


Figura 37: Alice y Bob obtienen sus claves.

Como se demostró en el Capítulo 4, la clave construida de esta manera es aproximadamente el 50% de la cantidad de bits enviados, en el formulario vemos que se obtuvo el 50.17%, es decir una clave de 24081 bits. A esta clave se le denomina "Clave sin procesar" o "clave en bruto (raw key)" porque todavía no se le ha aplicado las operaciones para calcular el QBER ni la corrección de errores.

Alice selecciona aleatoriamente la mitad de bits de sus claves sin procesar[51] y publica sus posiciones y polarizaciones por un canal clásico, Bob usando las mismas posiciones publica las polarizaciones correspondiente, de esta manera se sacrifica esta cantidad de bits, en este ejemplo 12040, ambos comparan y calculan el QBER, como se esperaba, en un sistema ideal sin espía y sin ruido, el QBER es igual a 0.00%.

Para calcular el QBER se eligió aleatoriamente los bits, entonces esto indica que la otra mitad de bits que solo conocen Alice y Bob tiene probablemente el mismo QBER. En la Figura 37 vemos en los paneles de la derecha las claves procesadas de Alice y Bob, que son de longitud 12401.

Como el QBER que se obtuvo es 0% entonces no tiene sentido corregir las claves y se procede a enviar el mensaje, clic el botón "Encriptar" para convertir el mensaje secreto a bits y realizar la operación XOR con la clave procesada de Alice y enviar el resultado a Bob por un medio clásico (Figura 38).

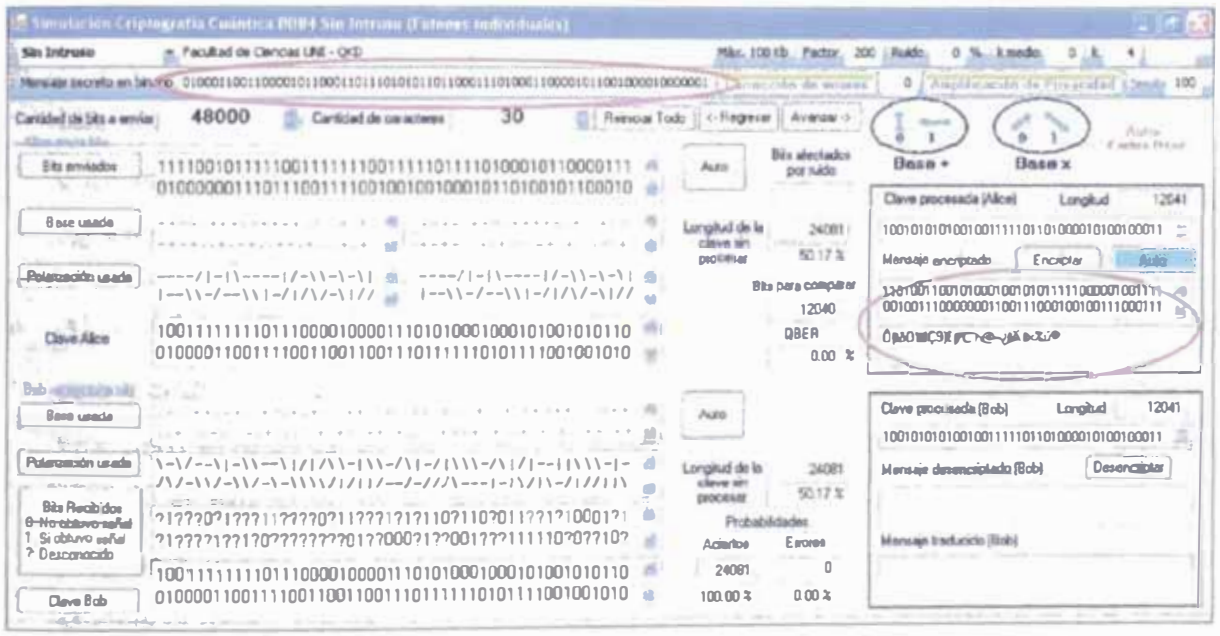


Figura 38: Alice encripta el mensaje.

En el panel de la derecha de la Figura 38 se muestra el mensaje encriptado en binario y su equivalente en código *ASCII*, como se observa el texto esta encriptado y es irreconocible.

Finalmente Bob recibe los bits y los desencripta aplicando nuevamente el operador XOR al mensaje encriptado con su clave (Figura 39).

[51] Si el número N de bits de la clave sin procesar es impar el programa selecciona para comparar la mitad de N-1.

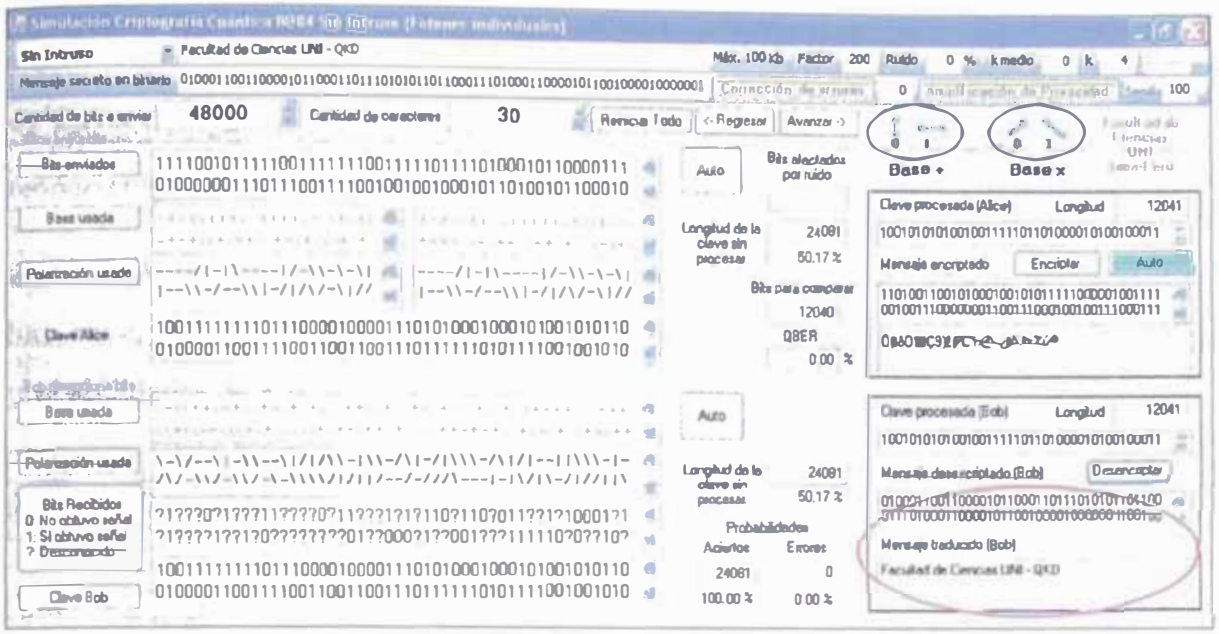


Figura 39: Bob desencripta el mensaje secreto.

De esta forma se envía con éxito cualquier mensaje utilizando el protocolo BB84.

Observaciones adicionales:

- El programa hace un análisis de la clave obtenida El cuadro "Aciertos" contiene los bits que coinciden con los de Alice, como no hubo ruido ni espías entonces corresponde al 100%. El cuadro "Errores" contiene los bits que no coinciden con los de Alice, como no hubo ruido ni espías entonces resulta 0%.

- Al principio se mencionó que bastan 8 bits por carácter para enviar el mensaje, en este ejemplo se tiene 30 caracteres, es decir que solo se necesita una clave de 240 bits, pero se observa que las claves procesadas tienen una longitud de 12041. Esto es porque al principio no se puede saber si hay ruido o espías, es por eso que el programa genera bits adicionales, la cantidad de bits adicionales dependerá de la eficiencia de los equipos que se utilicen, de las condiciones atmosféricas por donde viajan los fotones, etc. Sin embargo el programa siempre usa los primeros bits de la clave procesada para encriptar o desencriptar. Si se desea reducir o aumentar esta clave procesada simplemente se modifica el "Factor" en el formulario. Este "Factor" indica cuantas veces 8 bits se utilizará por carácter.

Esta simulación se realizó con éxito y con las probabilidades esperadas en la máquina de criptografía construida. En la máquina se utilizó un Factor de 2, más adelante se muestra estos resultados experimentales.

Gráfica de comparación con el valor teórico

Se ejecutó varias veces el programa, Tabla 2, y se graficó para comparar con el valor teórico (Figura 40).

En el Capítulo 4 se muestra que la clave es probabilísticamente el 50% de la cantidad de bits enviados por Alice y en el párrafo 4.1 se muestra que Bob tiene las siguientes probabilidades de acertar y equivocarse.

$$p_{acertar}^{Bob} = \frac{1}{2} + \frac{1}{2} = 100\%$$

$$p_{equivocar}^{Bob} = 0\%$$

$$QBER = 0\%$$

Mensaje secreto a enviar: Facultad de Ciencias

Cantidad de bits a enviar: 32000

Sin espías sin ruido							
Simulación	Alice			Bob			QBER %
	Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %	
1	32000	16056	50.18	16056	50.18	100.00	0.00
2	32000	15940	49.81	15940	49.81	100.00	0.00
3	32000	16152	50.48	16152	50.48	100.00	0.00
4	32000	15986	49.96	15986	49.96	100.00	0.00
5	32000	16137	50.43	16137	50.43	100.00	0.00
6	32000	15911	49.72	15911	49.72	100.00	0.00
7	32000	15923	49.76	15923	49.76	100.00	0.00
8	32000	16015	50.05	16015	50.05	100.00	0.00
9	32000	16078	50.24	16078	50.24	100.00	0.00
10	32000	15969	49.90	15969	49.90	100.00	0.00

Teóricamente	Alice			Bob			QBER %
	Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %	
1	32000	16000	50.00	16000	50.00	100.00	0.00
2	32000	16000	50.00	16000	50.00	100.00	0.00
3	32000	16000	50.00	16000	50.00	100.00	0.00

4	32000	16000	50.00	16000	50.00	100.00	0.00
5	32000	16000	50.00	16000	50.00	100.00	0.00
6	32000	16000	50.00	16000	50.00	100.00	0.00
7	32000	16000	50.00	16000	50.00	100.00	0.00
8	32000	16000	50.00	16000	50.00	100.00	0.00
9	32000	16000	50.00	16000	50.00	100.00	0.00
10	32000	16000	50.00	16000	50.00	100.00	0.00

Tabla 2: Datos simulados sin espía y sin ruido.

En la Tabla 2, al no haber ruido ni espías Bob acierta el 100% de la clave y por tanto el QBER es cero.

Al ser un proceso aleatorio en cada simulación se obtiene una longitud de la clave alrededor del 50% de la cantidad de bits enviados por Alice, tal como predice la teoría. En la Figura 40 se muestra un gráfico comparativo.

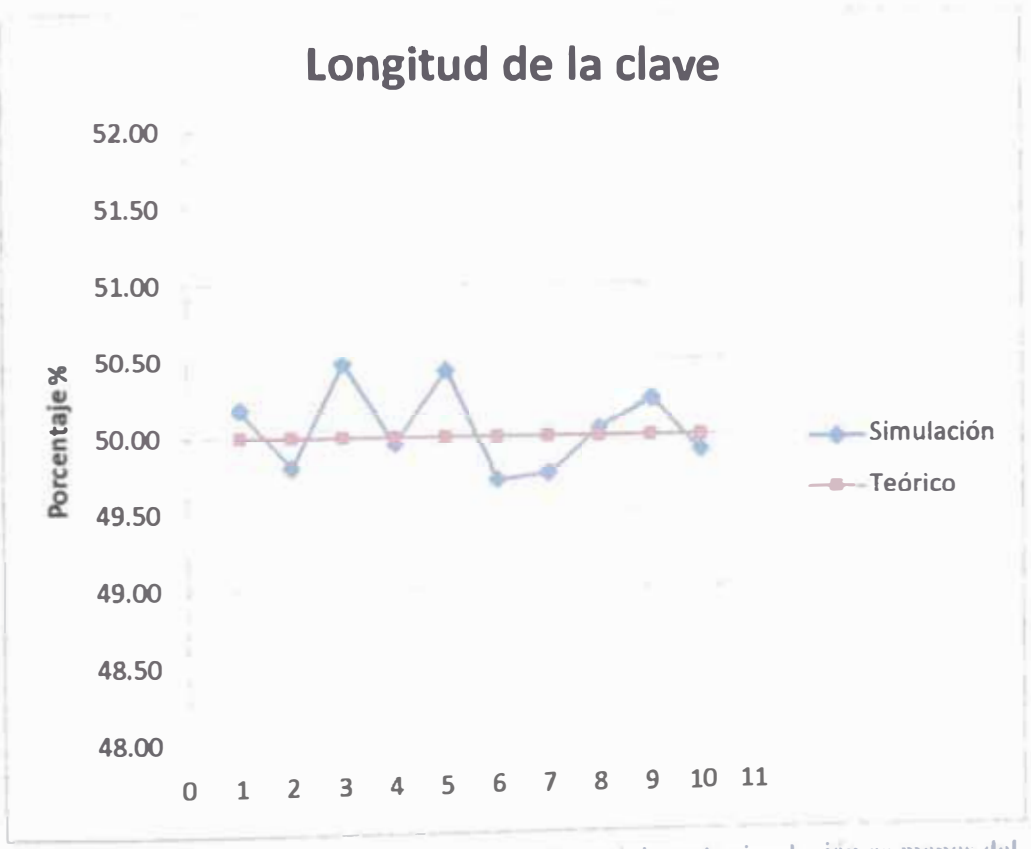


Figura 40: La diferencia máxima entre el valor teórico y la simulación es menos del 0.5%.

5.3 Simulación de transmisión con un ruido δ% y sin espia

En la simulación, si un bit es afectado por el ruido entonces su polarización se cambiará por su ortogonal o cualquiera de las polarizaciones de su base conjugada.

Se ejecuta el programa BB84.exe para generar una clave para enviar el mensaje secreto "Facultad de Ciencias UNI - QKD" que tiene 30 caracteres. Es decir que Alice enviará 48 mil fotones.

Por ejemplo, si el ruido es del 30%, en el cuadro "Ruido" se escribe 30 y se realiza los mismos pasos del párrafo 5.2, se obtiene un QBER de 20.10% (Figura 41).

El cuadro "k medio" indica que si los errores estuvieran distribuidos uniformemente, entonces aproximadamente 2414 bloques de 4 bits tendrían un bit erróneo[52].

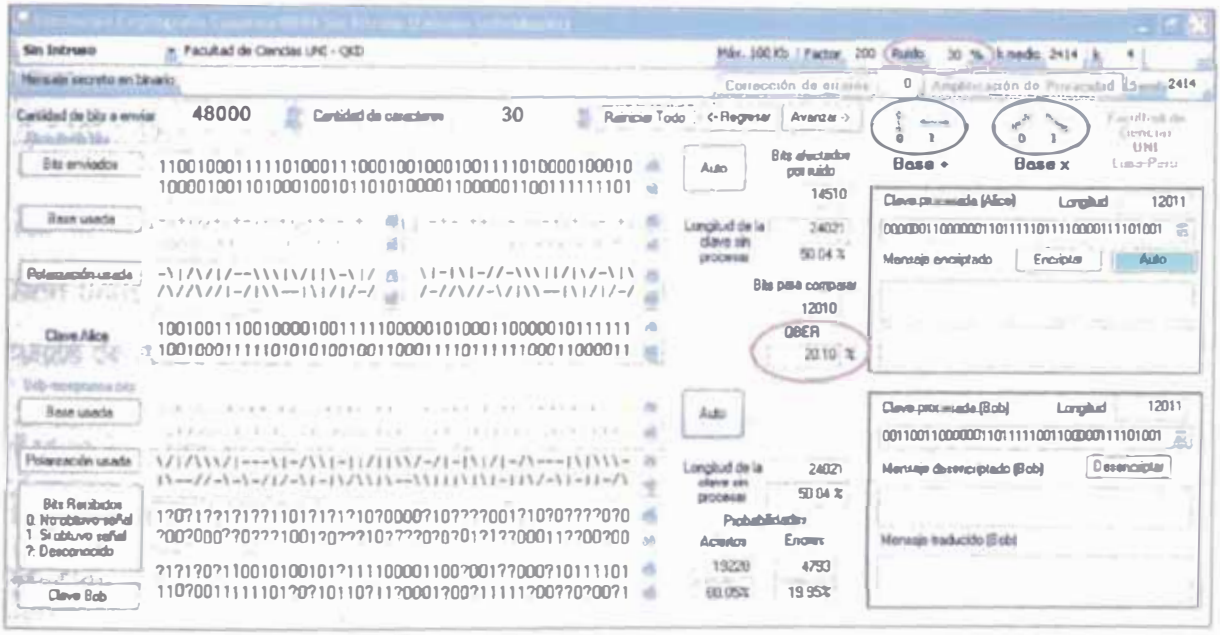


Figura 41: Un ruido de 30% genera un QBER aproximado de 20%. En la simulación se tiene 20.10%.

En la Tabla 3 se analiza los 8 primeros envíos, con fondo amarillo aparecen todos los fotones afectados, pero solo los de fuente roja formarán parte de la clave porque corresponden a bases iguales de Alice y Bob

[52] Esta información se refiere a toda la clave, obviamente este dato no la poseen ni Alice ni Bob, pues ambos publican solo la mitad de sus claves, esta información se colocó como dato informativo estadístico durante la escritura del programa y se puede retirar sin causar problema.

Envío		1	2	3	4	5	6	7	8
Bits generados por Alice		1	1	0	0	1	0	0	0
Alice envía	Base	+	×	+	×	×	×	+	×
	Polarización	–	\	|	/	\	/	|	/
Efecto del ruido	Base	×	+	+	+	×	+	+	×
	Polarización	\	|	–	|	\	|	–	/
Bob recepciona	Base	×	×	+	×	×	×	×	×
	Polarización	\	/	|	/	\	\	\	/
	Medida	1	?	0	?	1	?	?	1

Clave Alice	1	0	0	1	0	0	. . .
Clave Bob	?	1	?	1	?	0	. . .

Tabla 3: Como ejemplo se analiza los primeros 8 bits para explicar cómo trabaja del software.

A continuación se analiza cada columna:

Envío 1: Alice envía una polarización – y el ruido lo cambia a la polarización \, como Bob mide con la polarización \ entonces su detector lo medirá (Medida = 1). Como las bases de Alice y Bob son distintas entonces el bit no formará parte de la clave.

Envío 2. Alice envía una polarización \ y el ruido la cambia a |, Bob mide con /, y tiene un 50% de que el fotón colapse a / (y su detector mediría la interacción con el fotón: Medida = 1) y tiene un 50% que colapse a \ (con lo que su detector no mediría nada: Medida = 0), lo que en el programa se denota por el signo **?** pues no se sabe con anticipación qué medida resultará. Además como Alice y Bob tiene la misma base ×, Alice toma el bit que representa \ como el primer bit de su clave (Clave Alice = 1). Por parte de Bob, su medida es **?**, entonces no se sabe que medirá ni tampoco se sabe que bit formará su clave (Clave Bob = ?).

Envío 3: Alice envía una polarización | y el ruido lo cambia a –, Bob utiliza | para medir y bloquea el fotón (Medida = 0), como Alice y Bob usan la misma base entonces

Alice toma el bit que representa | para añadir a su clave (Clave Alice = 10). Bob no logro medir el fotón entonces el supone que lo ha bloqueado y asume que la polarización que envió Alice es ortogonal a la de él, por tanto toma el bit que representa – y lo añade a su clave (Clave Bob = ?1), obteniendo un bit erróneo.

Envío 4: Alice envía una polarización / y el ruido la cambia a |, Bob mide con /, y tiene un 50% de que el fotón colapse a / (y su detector mediría la interacción con el fotón: Medida = 1) y tiene un 50% que colapse a \ (con lo que su detector no mediría nada: Medida = 0), por eso el programa muestra el signo **?** para denotar que no se sabe con anticipación qué medida resultará. Además como Alice y Bob tiene la misma base ×, Alice toma el bit que representa / como el primer bit de su clave (Clave Alice = 100). Por parte de Bob, su medida es ?, entonces no se sabe que medirá ni tampoco se sabe que bit formará su clave (Clave Bob = ?1?).

Envío 5. Alice envía una polarización \ y no es afectado por el ruido, Bob utiliza \ para medir y detecta el fotón (Medida = 1) Como ambos usaron la misma base, Alice añade el bit que representa \ a su clave (Clave Alice = 1001). Por su parte Bob, como detecto el fotón el supone que acertó la polarización de Alice y utiliza el bit que representa \ a su clave (Clave Bob = ?1?1).

Envío 6: Alice envía una polarización / y el ruido la cambia a |, Bob mide con \, y tiene un 50% de que el fotón colapse a \ (y su detector mediría la interacción con el fotón: Medida = 1) y tiene un 50% que colapse a / (con lo que su detector no mediria nada: Medida = 0), por eso el programa muestra el signo **?** para denotar que no se sabe con anticipación qué medida resultará. Además como Alice y Bob tiene la misma base ×, Alice toma el bit que representa / como el primer bit de su clave (Clave Alice = 10010). Por parte de Bob, su medida es **?**, entonces no se sabe que medirá ni tampoco se sabe que bit formará su clave (Clave Bob = ?1?1?).

Envío 7: Alice envía una polarización | y el ruido lo cambia a –, como Bob mide con la polarización \ entonces tiene un 50% de detectarlo y un 50% de no detectarlo (Medida = **?**). Como las bases de Alice y Bob son distintas entonces el bit no formará parte de la clave.

Envío 8: Alice envía una polarización / y no es afectado por el ruido, Bob utiliza / para medir y detecta el fotón (Medida = 1). Como ambos usaron la misma base, Alice añade el bit que representa / a su clave (Clave Alice = 100100). Por su parte Bob, como detecto el fotón el supone que acertó la polarización de Alice y utiliza el bit que representa / a su clave (Clave Bob = ?1?1?0).

De forma similar funciona el resto de los envíos de Alice. Al terminar de construir la clave, el programa obtiene un QBER de 20.10%, entonces se procede a la corrección de errores. Clic al botón "Corrección de errores" y el programa encuentra 1267 bloques con paridad distinta los cuales son eliminados (Figura 42).

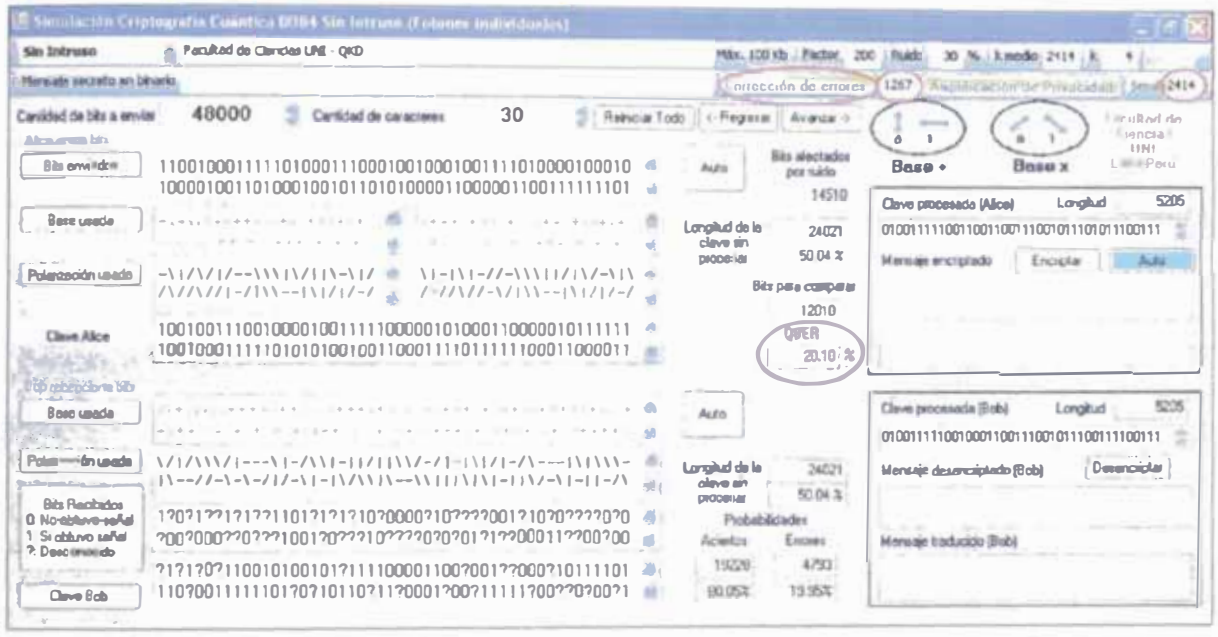


Figura 42: Primera corrección de errores, se encontró 1267 bloques de paridad distinta.

El algoritmo de corrección de errores antes de dividir la clave sin procesar en bloques de cuatro bits, primero permuta los bits de las claves de Alice y Bob de manera aleatoria, usando ambos la misma semilla. Esta semilla es el valor que aparece en el cuadro "Semilla" que el programa toma como valor inicial para ir generando más semillas. Este valor puede ser cualquiera y se ha tomado arbitrariamente igual al valor que aparece en el cuadro "k medio".

Otra vez se hace clic al botón "Corrección de errores" y se obtiene 456 bloques distintos, los que se eliminan (Figura 43).

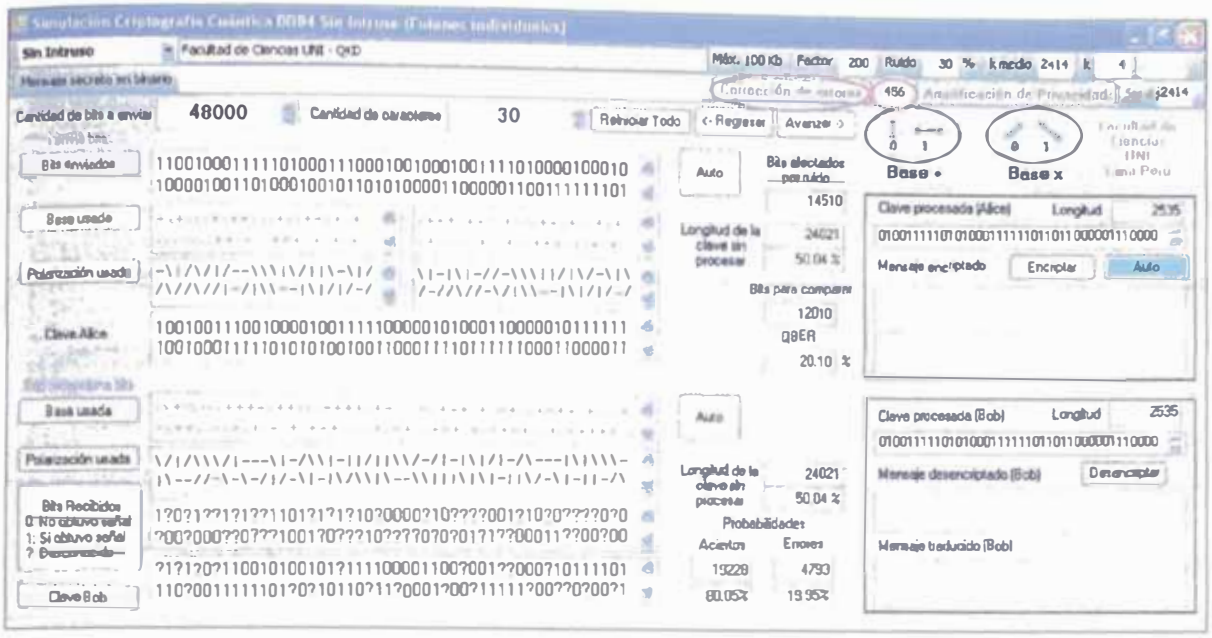


Figura 43: Segunda corrección de errores, se encontró 456 bloques de paridad distinta.

Otra vez clic al botón "Corrección de errores" y se obtiene 131 bloques distintos (Figura 44).

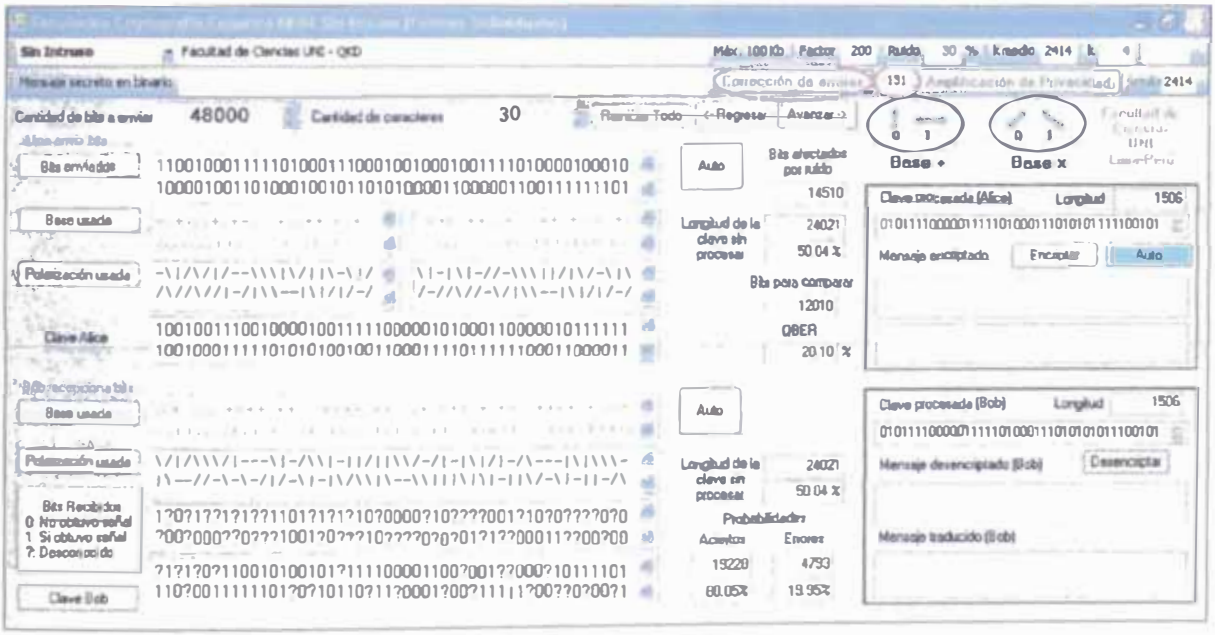


Figura 44: Tercera corrección de errores, se encontró 131 bloques de paridad distinta.

Otra vez clic al botón "Corrección de errores" y se obtiene 29 bloques distintos (Figura 45). Observe que a medida que se corrige los errores, la longitud de la clave procesada va disminuyendo, esto es debido a que cada bloque de distinta paridad se elimina y además a cada bloque de igual paridad se le quita el último bit.

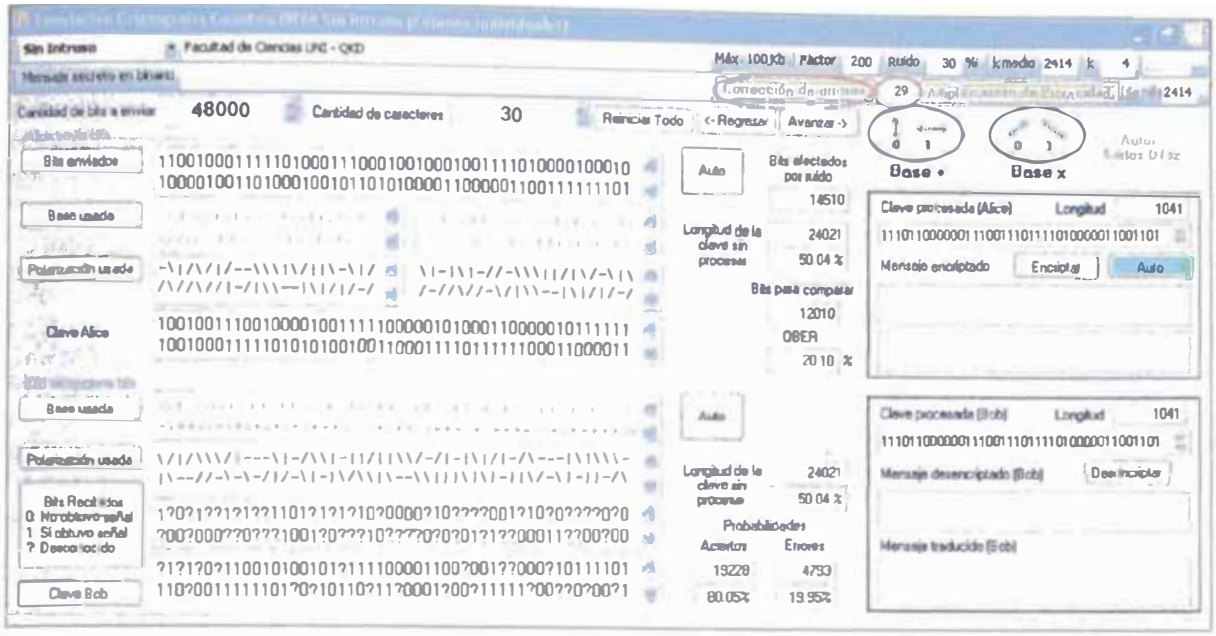


Figura 45: Cuarta corrección de errores, se encontró 29 bloques de paridad distinta.

Otra vez clic al botón "Corrección de errores" y se obtiene 1 bloque distinto (Figura 46).

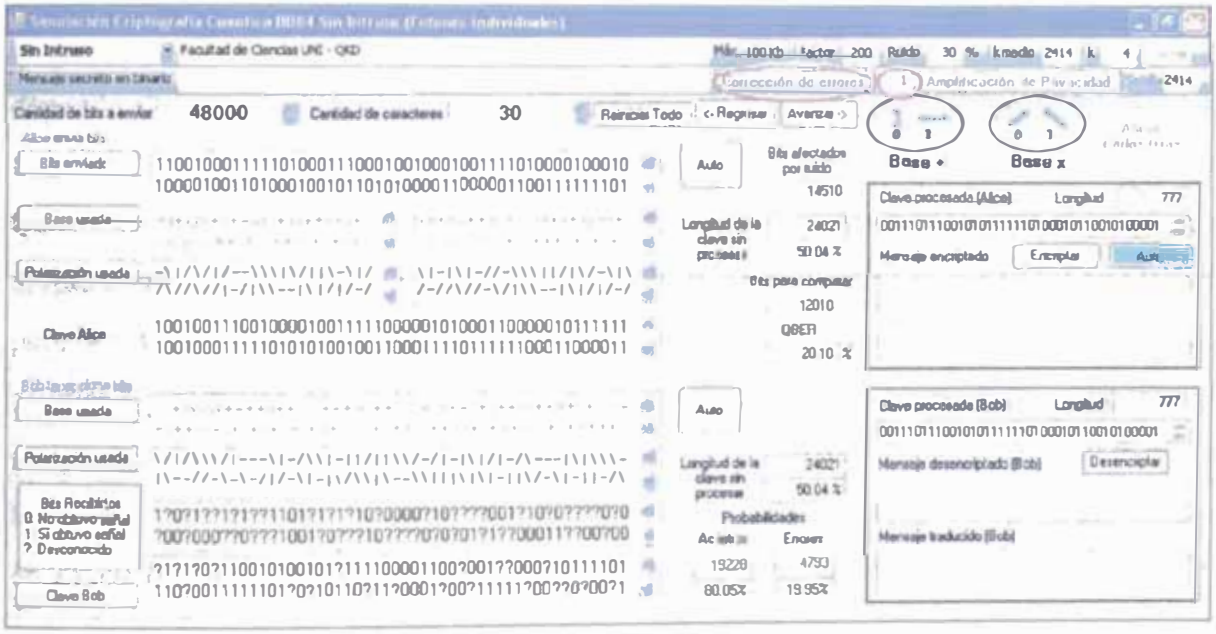


Figura 46: Quinta corrección de errores, se encontró 1 bloque de paridad distinta.

Otra vez clic al botón "Corrección de errores" y ya no se encuentra bloques con paridad distinta (Figura 47).

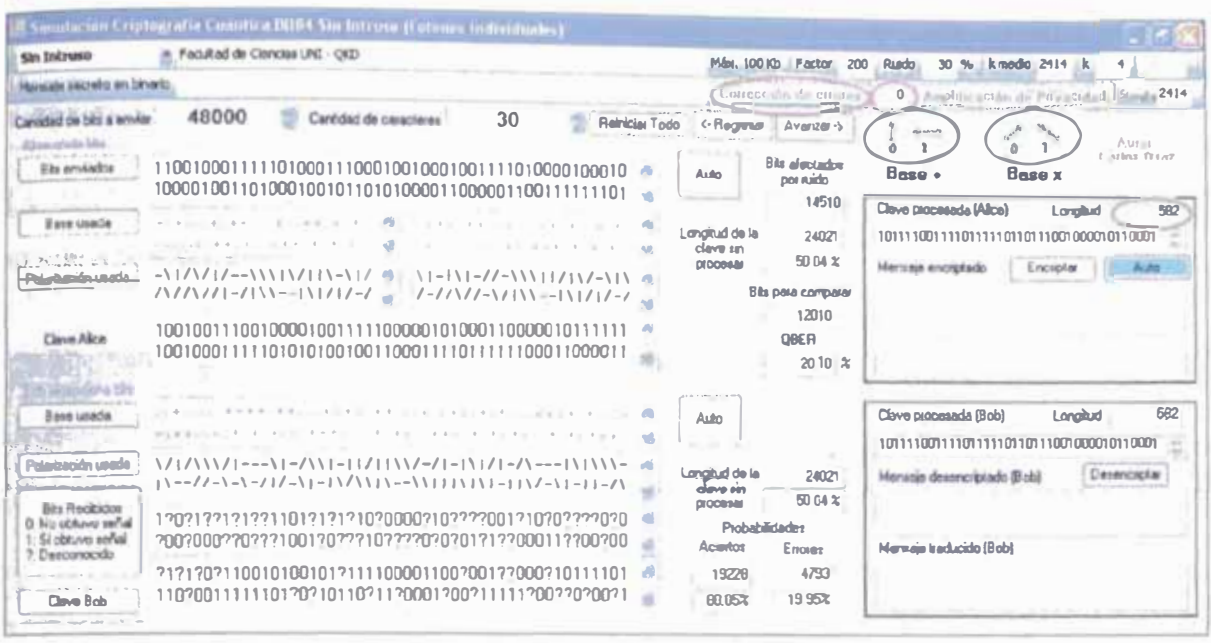


Figura 47: Sexta corrección de errores, ya no se encuentran bloques de paridad distinta.

En este punto ya se puede amplificar la privacidad pero existe una mínima posibilidad que dos bloques parezcan iguales y en realidad sean diferentes, esto sucede cuando en un bloque se tiene dos bits erróneos[53], por eso se recomienda hacer una corrección más depende de cuantos bits queden para sacrificar, en este ejemplo quedan 582 bits y se necesita 30 × 8 = 240 bits para enviar el mensaje y 240 bits más para calcular el último QBER, es decir se necesita 480 bits. Pero si se realiza una corrección más el programa dividirá 582 en bloques de 4, de los cuales eliminará el último bit, entonces quedarían para la clave 582 - 582/4 = 437 bits y faltarían 480 - 437 = 43 bits para tener la longitud necesaria y faltarían aún más si es que se encuentran bloques distintos. Sin embargo el programa completaría los bits faltantes copiando los primeros bits de la clave al final de la misma, lo cual no es recomendable pues un análisis de frecuencia de un espía podría encontrar bloques de bits repetidos. Por ese motivo ya no se realiza ninguna corrección más y se procede a amplificar la privacidad. Clic al botón "Amplificación de privacidad" (Figura 48).

La amplificación de privacidad tiene por objetivo reducir la cantidad de bits correctos que pueda tener un espía, esto se logra realizando operaciones con bits aleatorios de Alice y Bob y reemplazando un bit aleatorio con el resultado, de tal forma que si el

[53] En este ejemplo esta posibilidad es mínima pues se están considerando bloques de 4 bits, sin embargo si se utilizará bloques de mayor longitud podría ocurrir este problema. Por ejemplo en 582 bits, se tiene 145 bloques de 4, la posibilidad que dos bits erróneos caigan en un solo bloque es 1/145 * 1/145 = 0.00476 %.

espía realiza las mismas operaciones existe la probabilidad de que mezcle un bit correcto con uno incorrecto obteniendo un resultado incorrecto y que reemplace un bit correcto por el resultado incorrecto y así aumenta su cantidad de bits erróneos.

La amplificación también puede aumentar el error de Bob si es que en su clave tiene algunos bits erróneos.

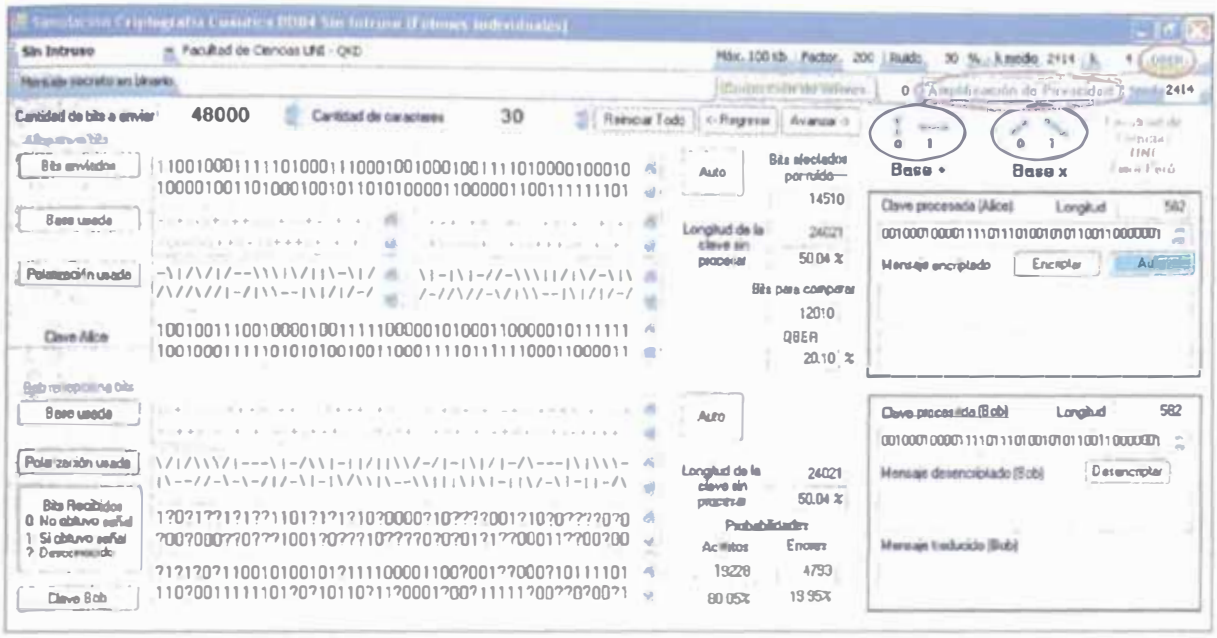


Figura 48: Amplificación de la privacidad, aumenta los bits erróneos de un posible espía.

Y ahora se presiona el botón "QBER" para hallar el nuevo QBER (Figura 49).

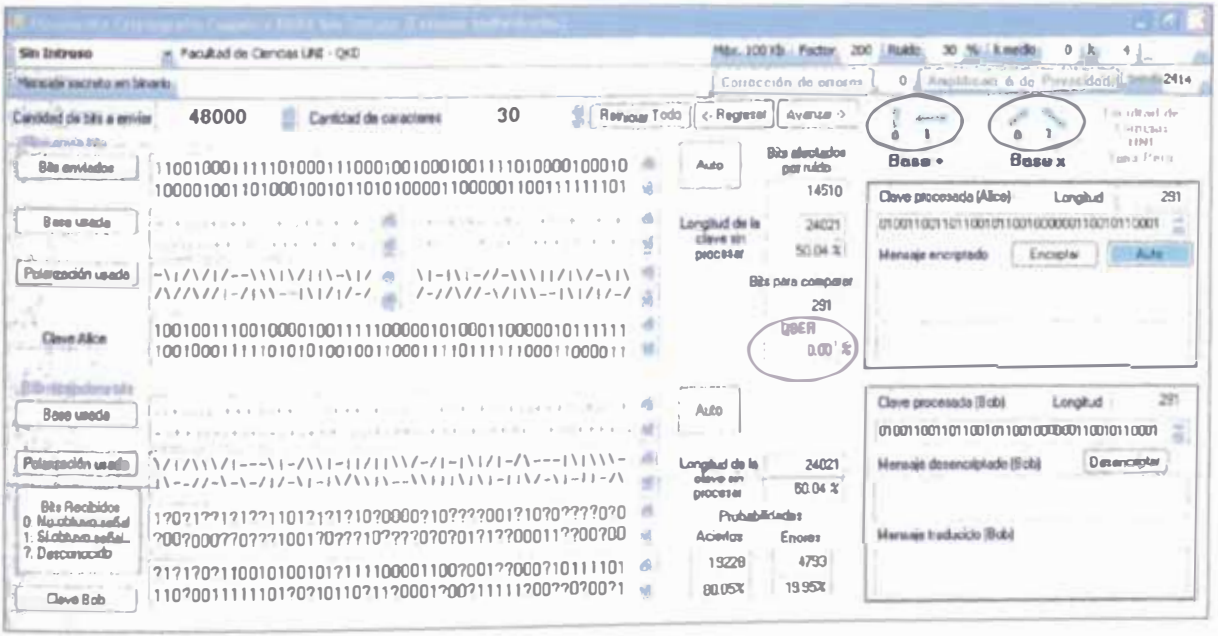


Figura 49: El QBER después de la corrección es cero.

El QBER resulta 0%, entonces ya se puede enviar el mensaje con seguridad, se presiona el botón "Encriptar" para enviar (Figura 50). Alice aplica la operación XOR al mensaje secreto en binario y a su clave procesada y envía el resultado a Bob por un canal clásico. Si un espía lo intercepta y convierte a código ASCII obtendría un mensaje ilegible.

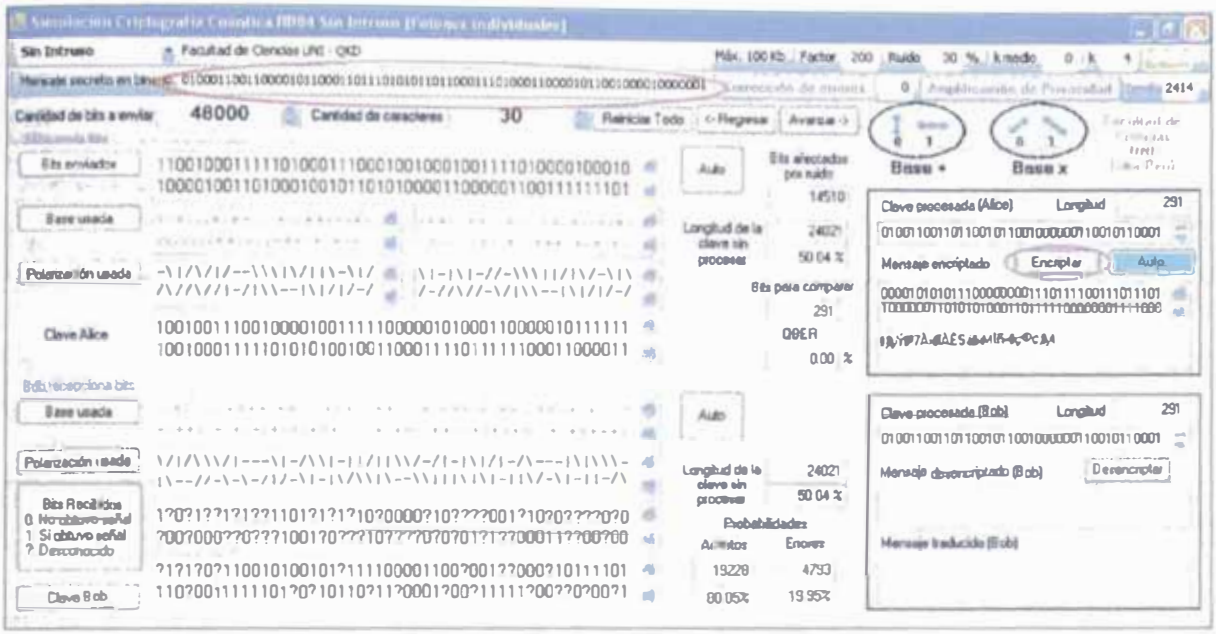


Figura 50: Para enviar el mensaje se hace clic al botón "Encriptar".

Finalmente Bob recibe el mensaje y lo desencripta presionado el botón "Desencriptar" (Figura 51). Bob aplica la operación XOR al mensaje en binario y a su clave procesada obteniendo el mensaje secreto.

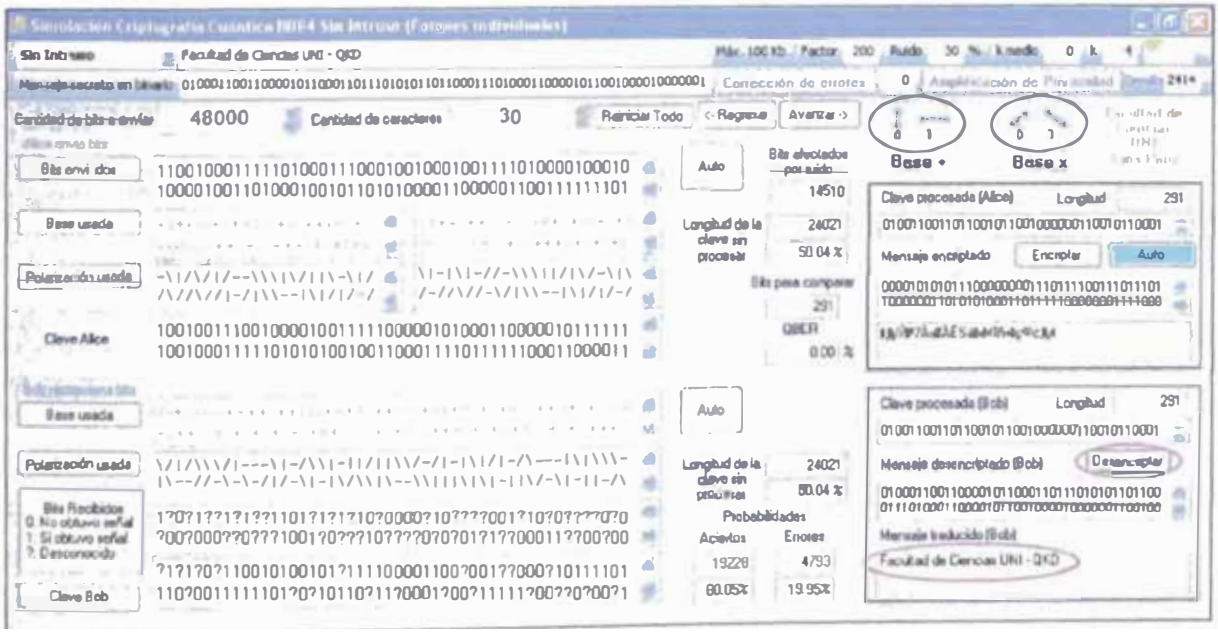


Figura 51: Para recibir el mensaje se hace clic al botón "Desencriptar".

De esta forma se demuestra como la simulación logra enviar un mensaje correcto incluso con ruido.

Pero cuál hubiese sido el resultado si no se hubiese corregido la clave.

Se tiene que ejecutar nuevamente el programa pues no se puede repetir las elecciones de Alice y Bob pues son aleatorias (Figura 52).

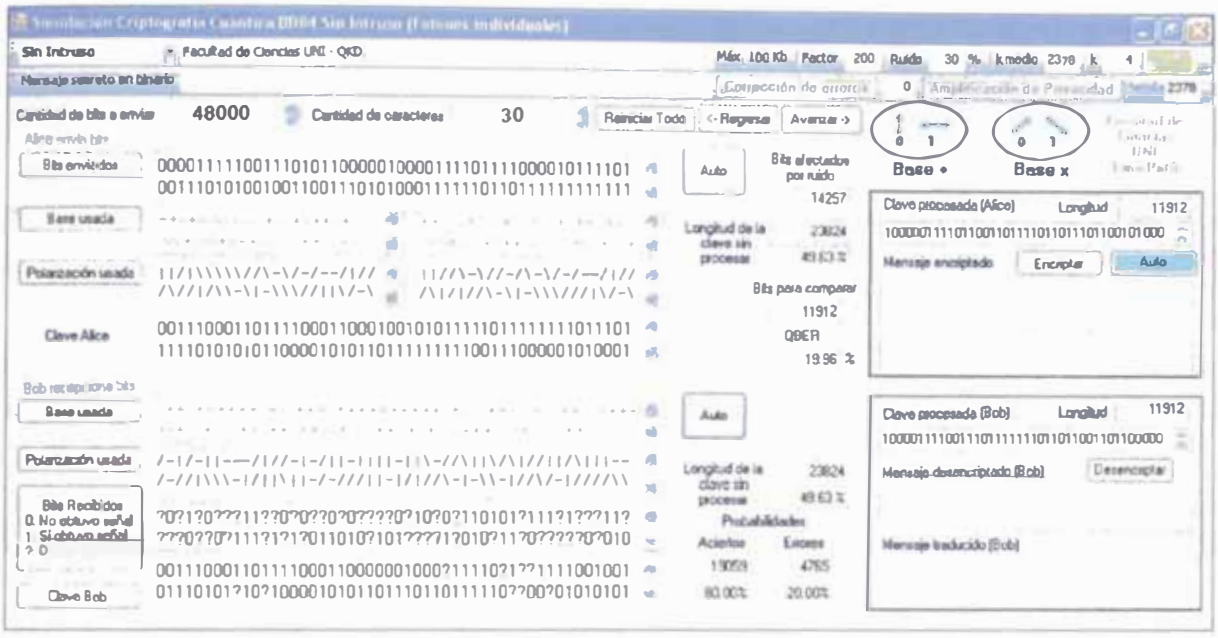


Figura 52: En esta ejecución se obtiene un QBER de 19.96%

Clic al botón "Encriptar" y "Desencriptar", el resultado en Bob es totalmente ilegible (Figura 53).

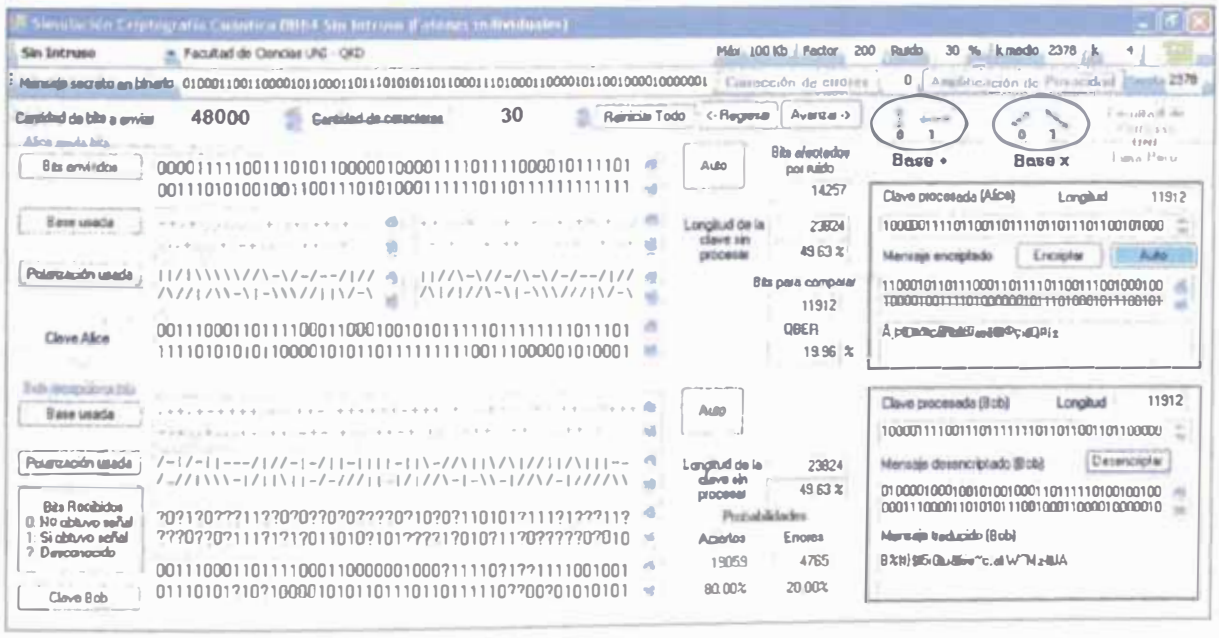


Figura 53: Sin la corrección de errores el mensaje recibido por Bob es ilegible".

Se observa cómo se van igualando las claves en cada corrección, obviamente esto no es lo que se hace en una transmisión real, el objetivo de las siguientes explicaciones es ver cómo funciona el protocolo internamente.

En la primera corrección todavía se sigue obteniendo un mensaje ilegible (Figura 54).

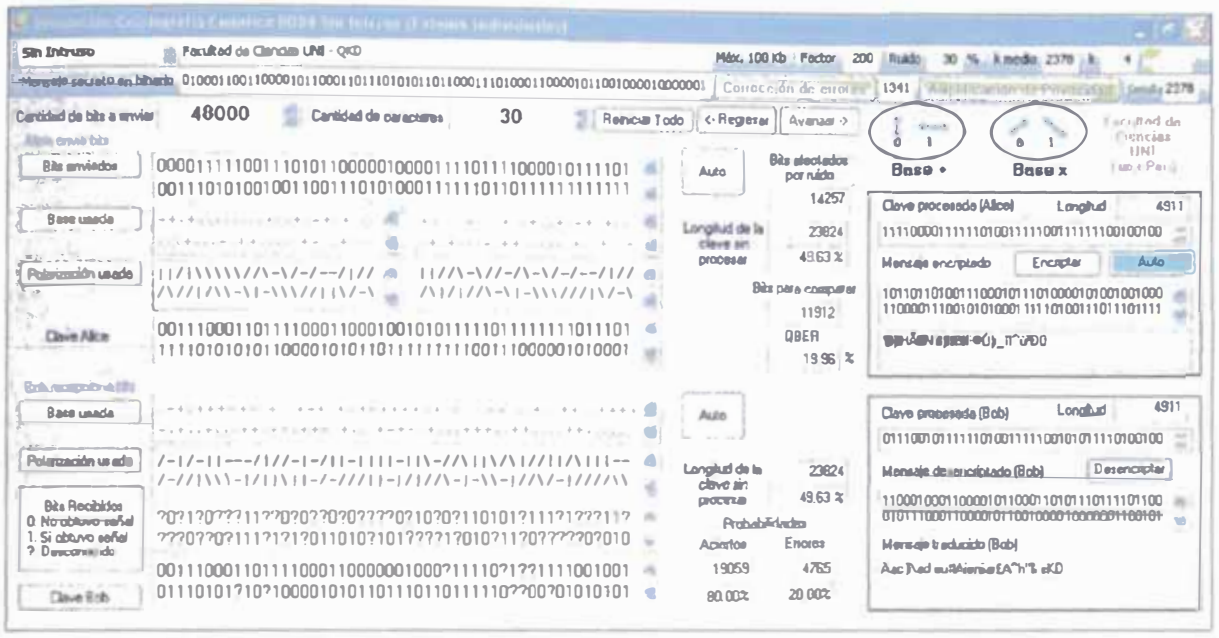


Figura 54: Primera corrección.

En la segunda corrección ya aparece la palabra "UNI" (Figura 55).

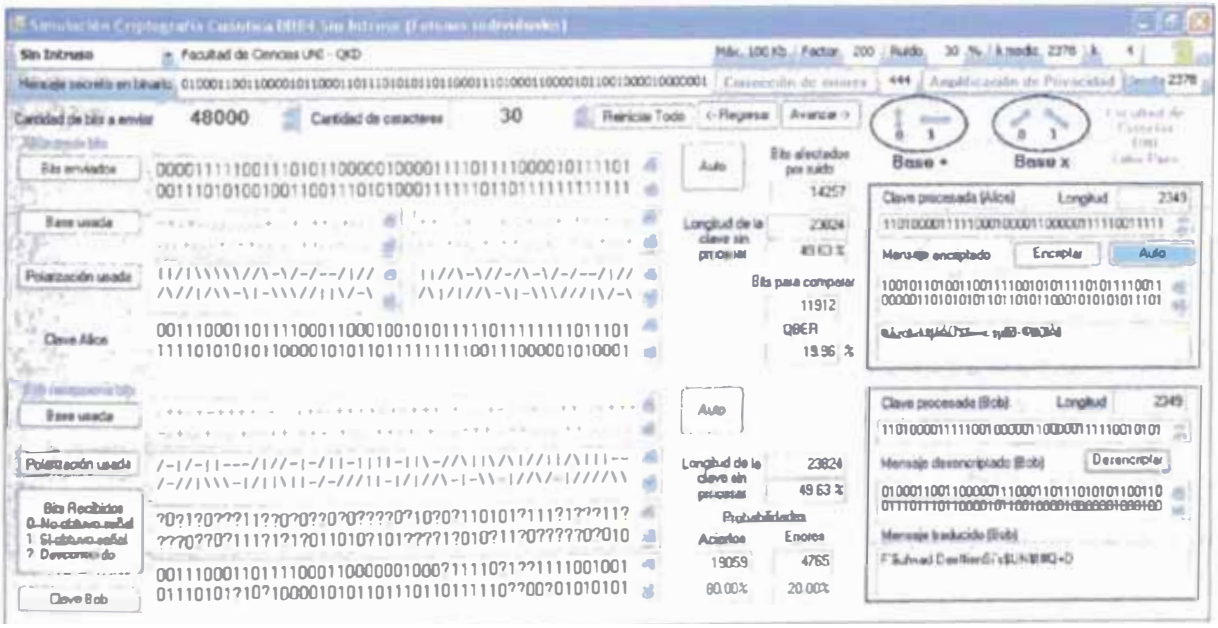


Figura 55: Segunda corrección.

En la tercera corrección aunque la palabra UNI ya no aparece, si aparece "QKD", además se puede intuir la palabra "Ciencias" (Figura 56).

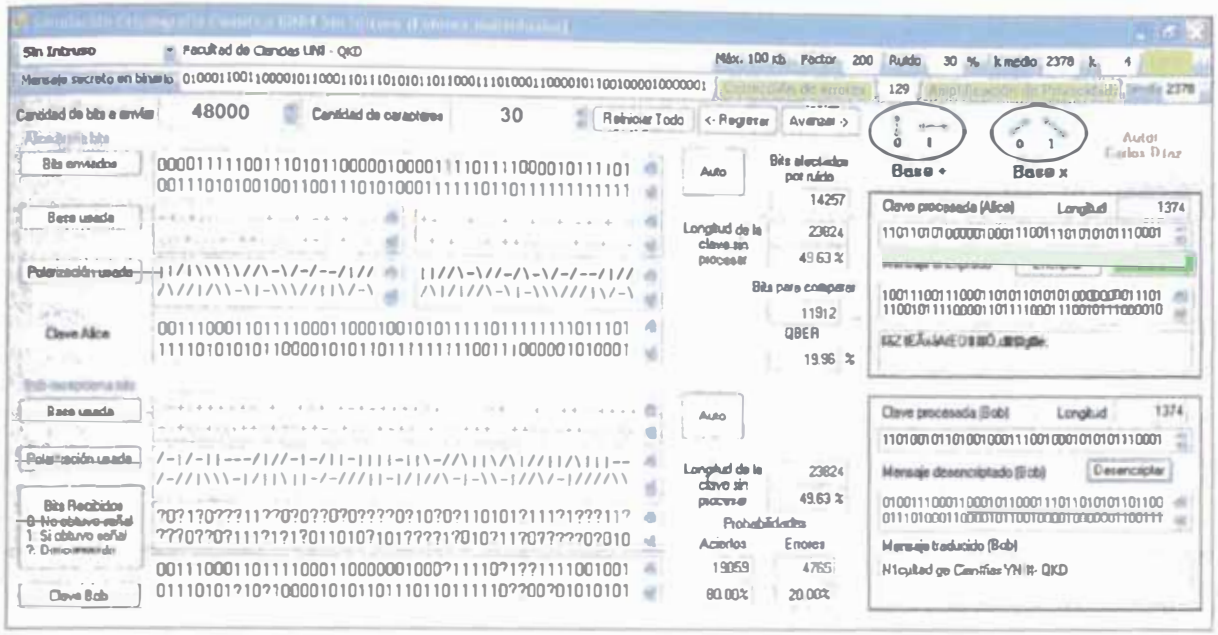


Figura 56: Tercera corrección.

En la cuarta corrección se obtiene un mensaje casi completo que se puede entender: Facultad de Ciencias UNI – QKD (Figura 57).

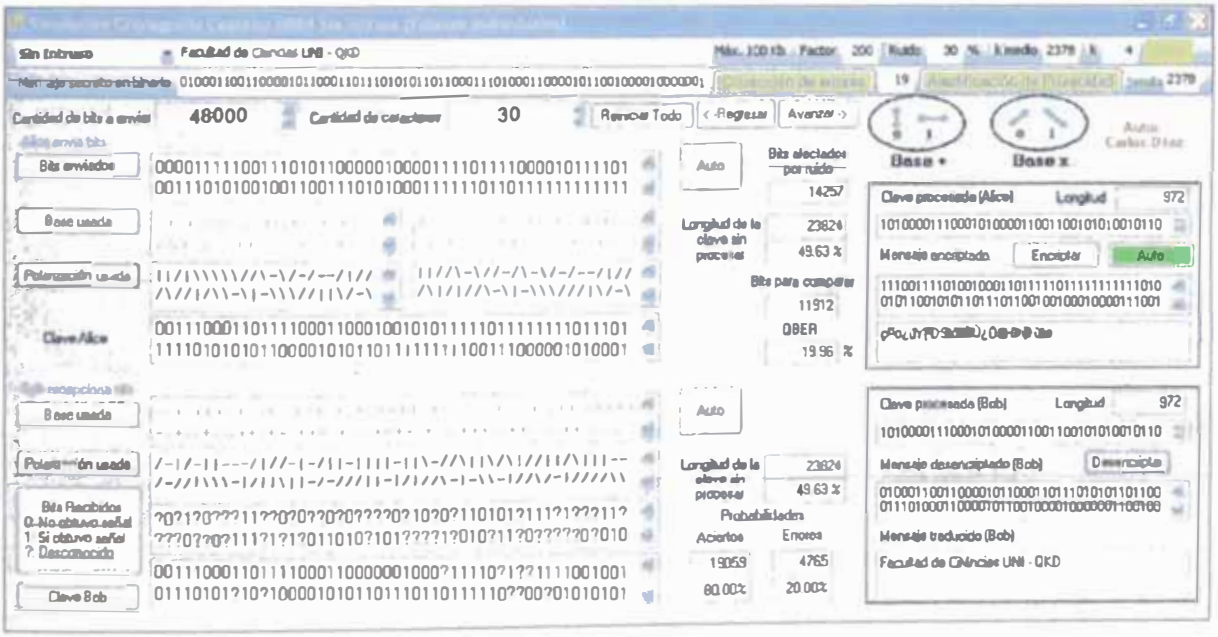


Figura 57: Cuarta corrección.

En la quinta corrección se obtiene el mensaje original (Figura 58).

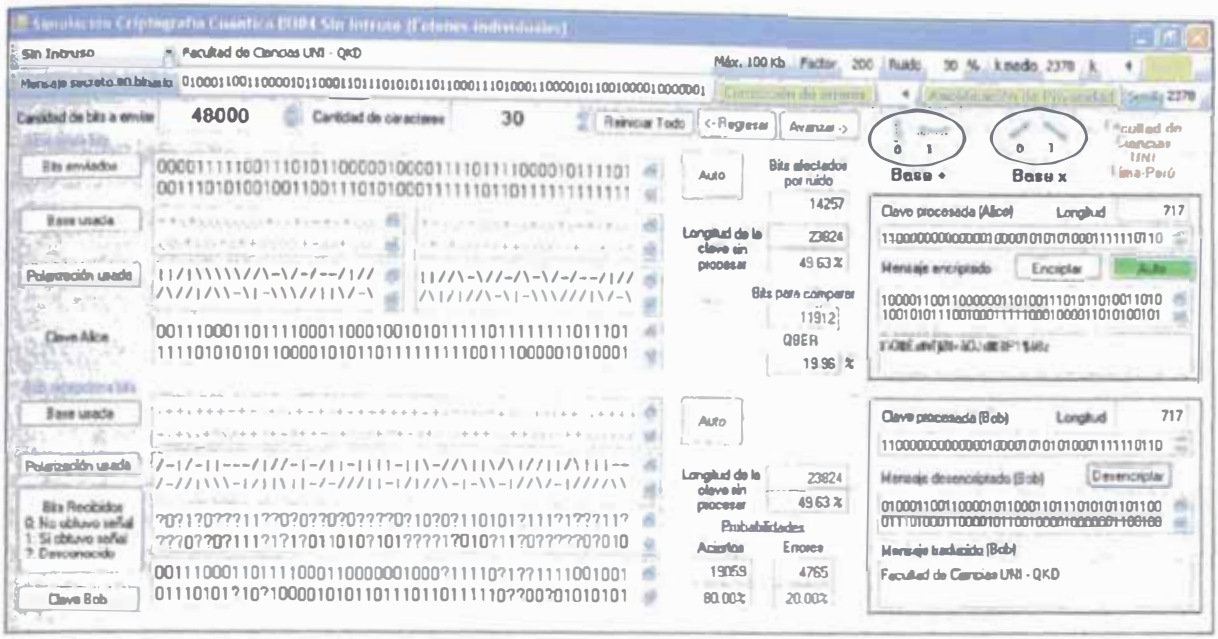


Figura 58: Quinta corrección.

En la sexta corrección ya no se encuentra paridades distintas y así concluye la corrección de errores (Figura 59).

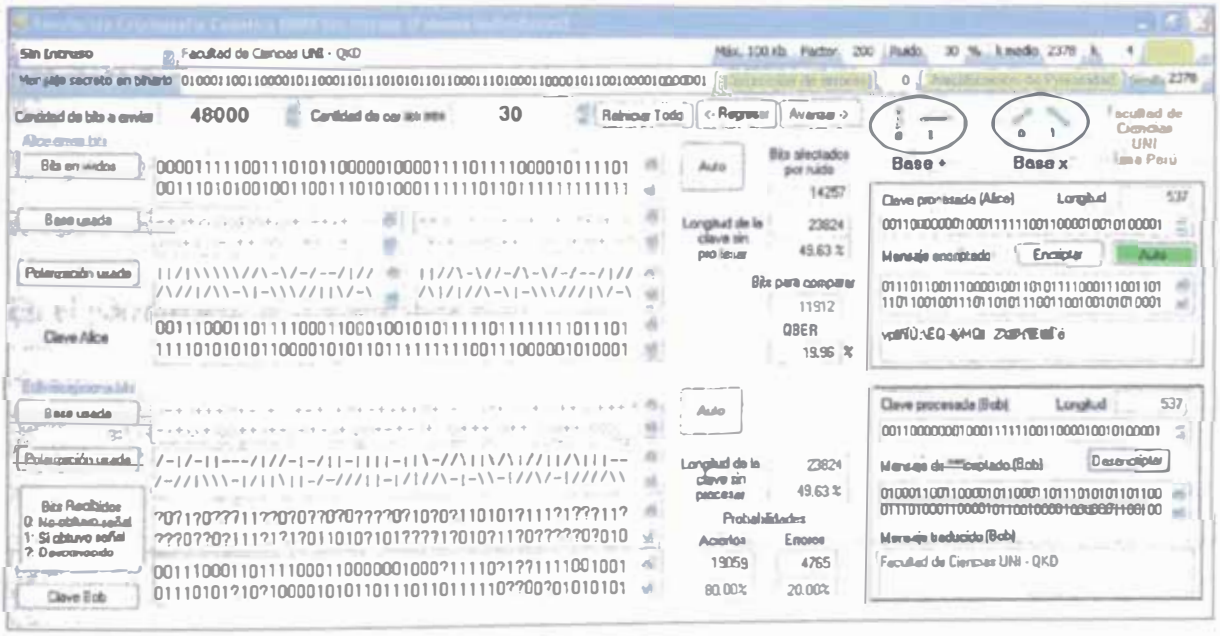


Figura 59: Sexta corrección.

Se amplifica la privacidad y se muestra el nuevo QBER, Alice encripta y Bob desencripta, como se esperaba, el resultado es correcto (Figura 60).

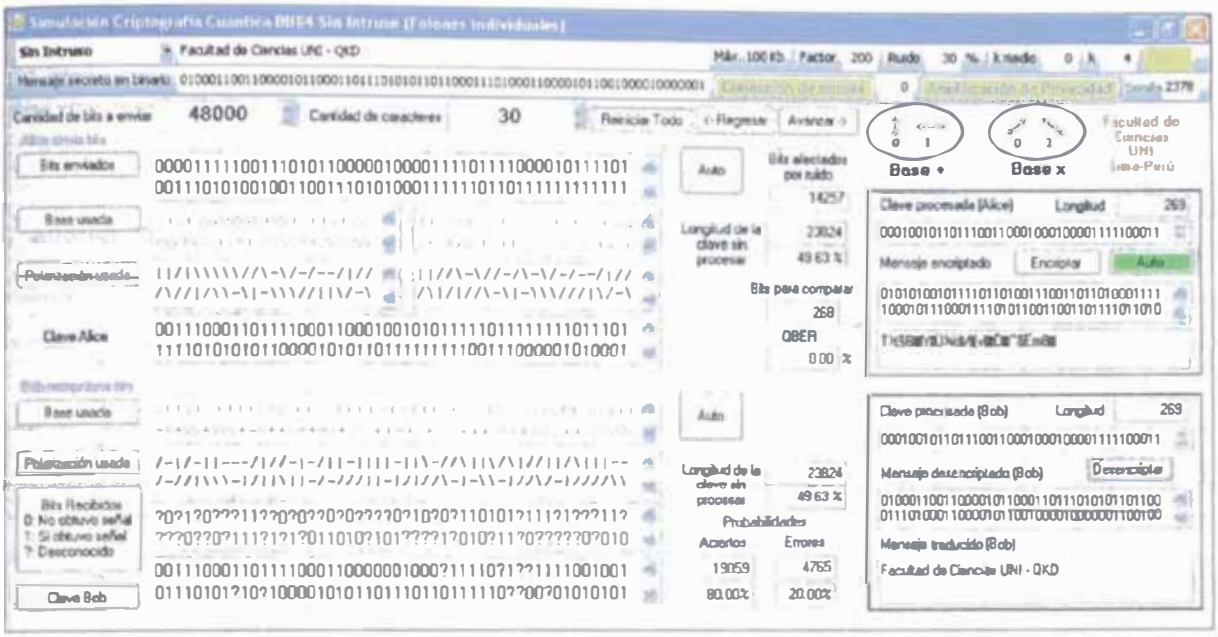


Figura 60: Amplificación de privacidad.

En cada corrección los bits de las claves de Alice y Bob se van igualando poco a poco, hasta obtener un QBER de 0%.

Gráfica de comparación con el valor teórico

Se ejecuto varias veces el programa, Tabla 4, y se realizo una gráfica para comparar con el valor teórico (Figura 61 y 62).

En el párrafo 4.4, se obtiene para Bob:

$$p_{acertar}^{Bob} = \frac{1}{3}\delta\% + (100-\delta)\% = \left(100 - \frac{2}{3}\delta\right)\%$$

$$p_{equivocar}^{Bob} = \frac{2}{3}\delta\%$$

$$QBER = \frac{2}{3}\delta\%$$

Mensaje secreto a enviar: Facultad de Ciencias

Cantidad de bits a enviar: 32000

Ruido δ: 30%

Ruido δ=30% sin espía								
Simulación	Ruido %	Alice			Bob			QBER %
		Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %	
1	30.00	32000	16078	50.24	16078	50.24	80.49	19.27
2	30.00	32000	16050	50.16	16050	50.16	79.86	19.96
3	30.00	32000	15923	49.76	15923	49.76	80.01	20.39
4	30.00	32000	15758	49.24	15758	49.24	79.89	20.26
5	30.00	32000	16124	50.39	16124	50.39	80.00	20.50
6	30.00	32000	16006	50.02	16006	50.02	80.00	20.55
7	30.00	32000	16107	50.33	16107	50.33	80.23	19.55
8	30.00	32000	16101	50.32	16101	50.32	80.20	19.58
9	30.00	32000	15943	49.82	15943	49.82	79.67	19.97
10	30.00	32000	15981	49.94	15981	49.94	79.67	20.20

Teóricamente	Ruido %	Alice			Bob			QBER %
		Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %	
1	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
2	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
3	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
4	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
5	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
6	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
7	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
8	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
9	30.00	32000	16000	50.00	16000	50.00	80.00	20.00
10	30.00	32000	16000	50.00	16000	50.00	80.00	20.00

Tabla 4: Datos simulados con ruido y sin espía.

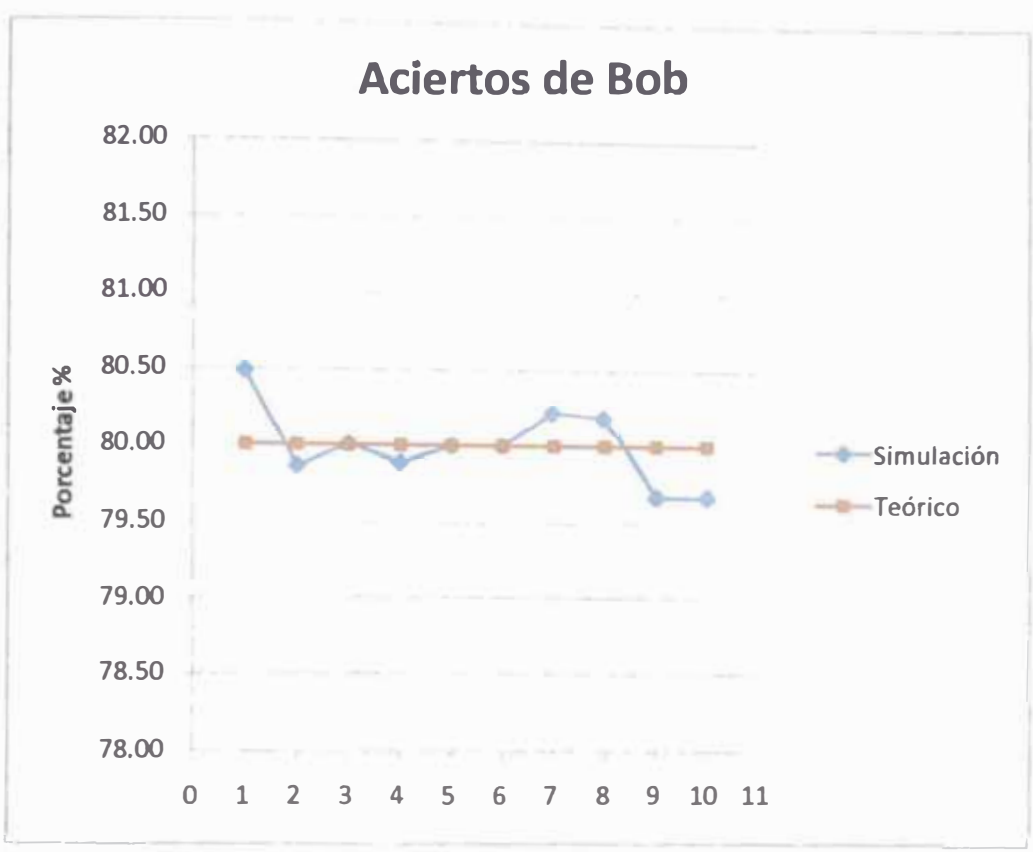


Figura 61: La diferencia máxima entre el valor teórico y la simulación es menos del 0.5%.

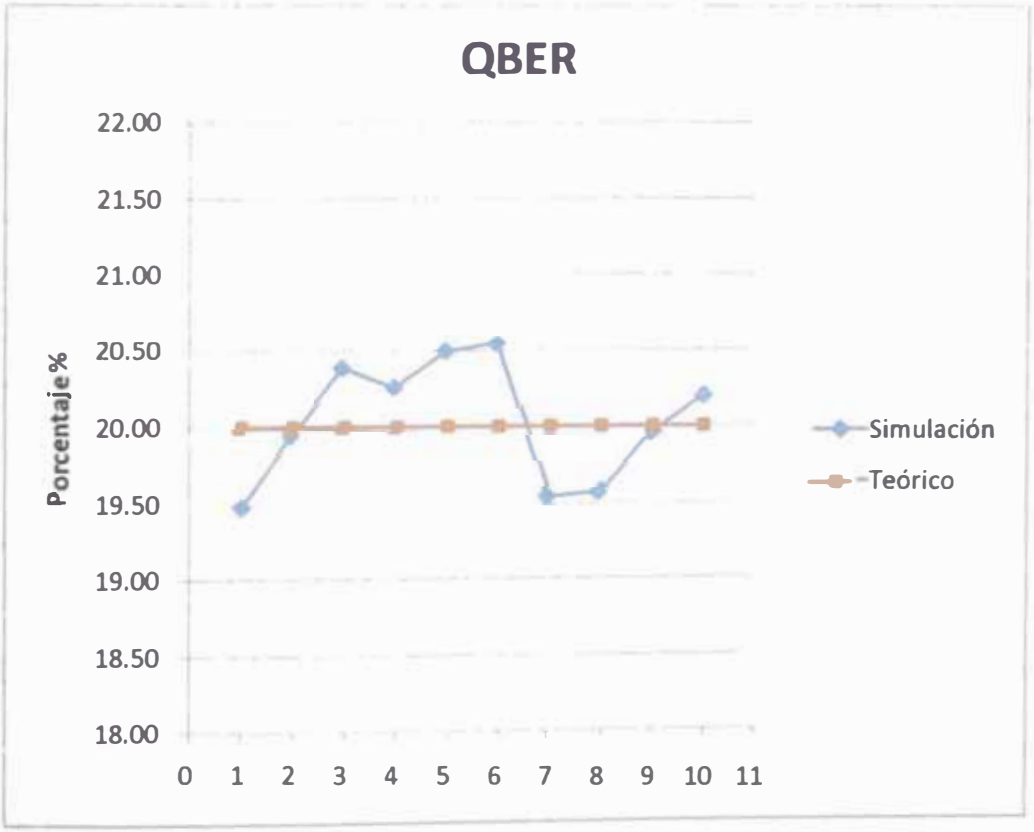


Figura 62: La diferencia máxima entre el valor teórico y la simulación es menos del 0.6%.

5.4 Simulación de transmisión con espía de intervención máxima y sin ruido (Man in the Middle)

En este caso el espía interviene todos los fotones enviados por Alice y reenvía a Bob un fotón con la polarización que midió. Este tipo de ataque es conocido como "Man in the Middle" (MITM) (37). En el programa se selecciona en la esquina superior izquierda la opción "Con Intruso (MITM)" (Figura 63).

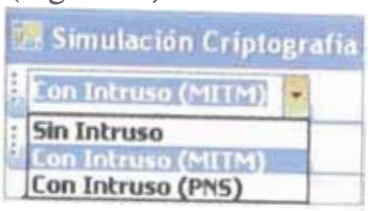


Figura 63: Del ListBox que se encuentra en la esquina superior izquierda se selecciona "Con Intruso (MITM).

Sea el mensaje secreto "Facultad de Ciencias UNI - QKD", tiene 30 caracteres y Alice enviará 48 mil fotones. Se ejecuta el programa, y se realiza pasos similares al párrafo 5.2, sólo que ahora aparece el espía Eve. Se obtiene un QBER de 25.23% (la teoría predice 25%, párrafo 4.2, fórmula 56), Bob obtiene un acierto de 74.95% (la teoría predice 75%, párrafo 4.2, fórmula 54) y Eve un acierto de 74,87 (la teoría predice 75%, párrafo 4.2, fórmula 55) (Figura 64).

Figura 64: Teóricamente Eve acierta el 75% de la clave (Simulación 74,87%), Bob acierta el 75% (Simulación 74,95%) y el QBER es 25% (Simulación 25,23%).

A pesar de que Eve tiene la probabilidad de acertar el 75% de la clave no significa que tiene el 75% de caracteres correctos, pues un carácter está formado por 8 bits, por tanto si Eve quiere obtener un carácter, tendrá que acertar 8 veces consecutivas de un conjunto de dos posibilidades (0 ó 1).

La probabilidad que Eve acierte un carácter es:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 75% = 0.29297%

En esta simulación Eve tiene una probabilidad de acertar un carácter de:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 74.87% = 0.29246%

A continuación se aplica la corrección de errores para ver si Bob logra obtener un mensaje legible, clic al botón "Corrección de errores" y "Amplificación de Privacidad" (Figura 65).

Figura 65: El QBER después de corregir y amplificar es 0.00% entonces es posible la comunicación entre Alice y Bob

Después de la corrección y amplificación el programa logra depurar las claves y obtener claves idénticas para Alice y Bob, sin embargo Eve no puede descubrir la clave y obtiene un mensaje ilegible si es que interviene el mensaje encriptado. Como se

menciono antes, nuestro programa corrige con seguridad hasta un QBER de 20% y con bastante probabilidad entre 20% y 25%.

Gráfica de comparación con el valor teórico

Se ejecuto varias veces el programa, Tabla 5, y se realizó una gráfica para comparar con el valor teórico (Figura 66, 67 y 68).

En el párrafo 4.2, se obtiene para Bob:

$$p_{acertar}^{Bob} = \frac{4}{8} + \frac{4}{16} = \frac{3}{4} = 75\%$$

$$p_{equivocar}^{Bob} = \frac{4}{16} = \frac{1}{4} = 25\%$$

$$QBER = 25\%$$

Y para Eve:

$$p_{acertar}^{Eve} = \frac{2}{4} + \frac{2}{8} = \frac{3}{4} = 75\%$$

$$p_{equivocar}^{Eve} = \frac{2}{8} = \frac{1}{4} = 25\%$$

Mensaje secreto a enviar: Facultad de Ciencias

Cantidad de bits a enviar: 32000

Interceptación máxima de un espía sin ruido										
Simulación	Alice			Bob			QBER %	Eve		
	Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %		Longitud	Porcent. %	Aciertos %
1	32000	16011	50.03	16011	50.03	75.17	24.93	16011	50.03	74.69
2	32000	16047	50.15	16047	50.15	75.27	24.84	16047	50.15	74.72
3	32000	16008	50.03	16008	50.03	74.43	25.55	16008	50.03	74.09
4	32000	15874	49.61	15874	49.61	75.07	25.43	15874	49.61	75.40
5	32000	16113	50.35	16113	50.35	74.75	25.56	16113	50.35	75.55
6	32000	15872	49.60	15872	49.60	75.17	24.62	15872	49.60	75.06
7	32000	15887	49.65	15887	49.65	75.02	25.20	15887	49.65	75.09
8	32000	16058	50.18	16058	50.18	75.46	25.02	16058	50.18	75.33
9	32000	15983	49.95	15983	49.95	74.75	25.29	15983	49.95	74.59
10	32000	16013	50.04	16013	50.04	75.23	24.88	16013	50.04	75.29

Teórica-mente	Alice			Bob			QBER %	Eve		
	Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %		Longitud	Porcent. %	Aciertos %
1	32000	16000	50.00	16000	50.00	75.00	25.00	16000	50.00	75.00
2	32000	16000	50.00	16000	50.00	75.00	25.00	16000	50.00	75.00
3	32000	16000	50.00	16000	50.00	75.00	25.00	16000	50.00	75.00
4	32000	16000	50.00	16000	50.00	75.00	25.00	16000	50.00	75.00
5	32000	16000	50.00	16000	50.00	75.00	25.00	16000	50.00	75.00
6	32000	16000	50.00	16000	50.00	75.00	26.00	16000	50.00	75.00
7	32000	16000	50.00	16000	50.00	75.00	27.00	16000	50.00	75.00
8	32000	16000	50.00	16000	50.00	75.00	28.00	16000	50.00	75.00
9	32000	16000	50.00	16000	50.00	75.00	29.00	16000	50.00	75.00
10	32000	16000	50.00	16000	50.00	75.00	30.00	16000	50.00	75.00

Tabla 5: Datos simulados con un espía máximo (λ=100%) y sin ruido.

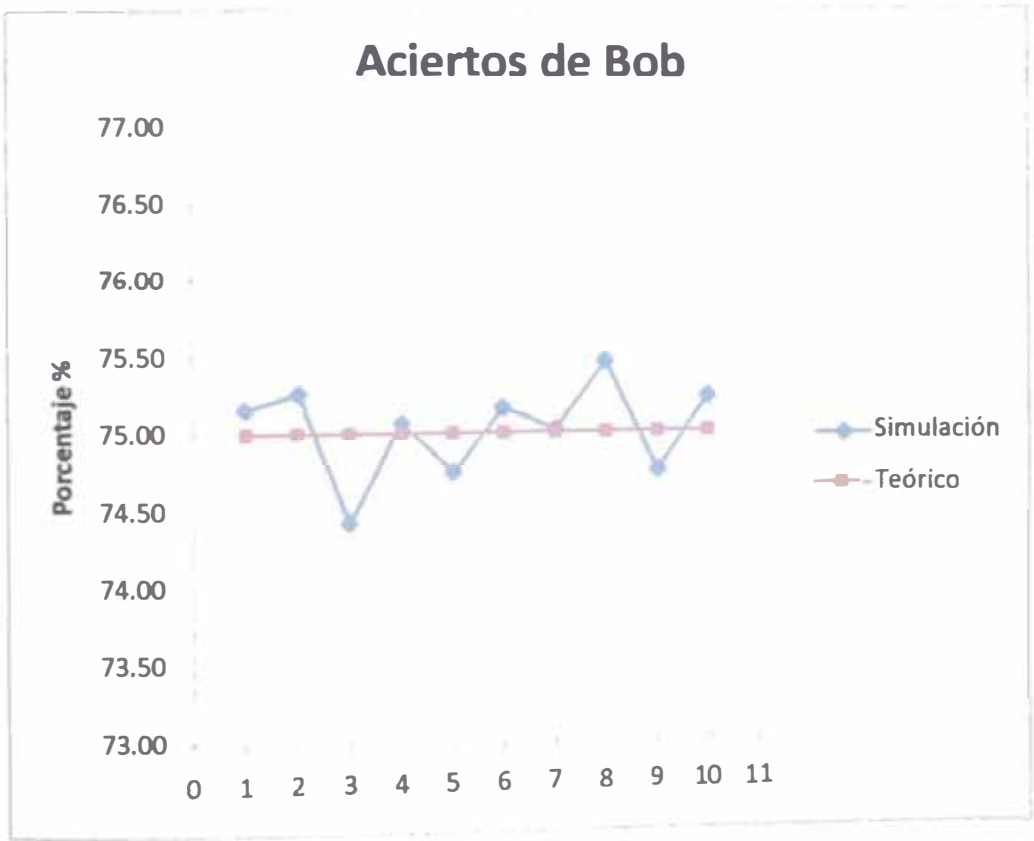


Figura 66: La diferencia máxima entre el valor teórico y la simulación es menos del 0.6%.

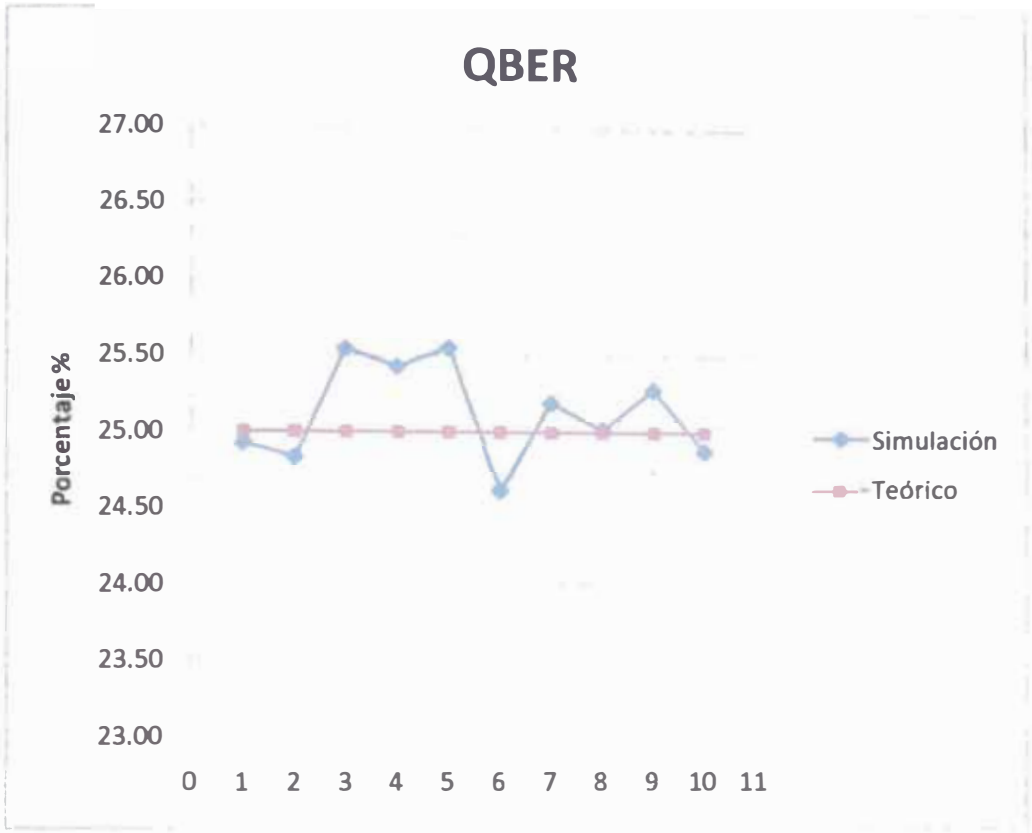


Figura 67: La diferencia máxima entre el valor teórico y la simulación es menos del 0.6%.

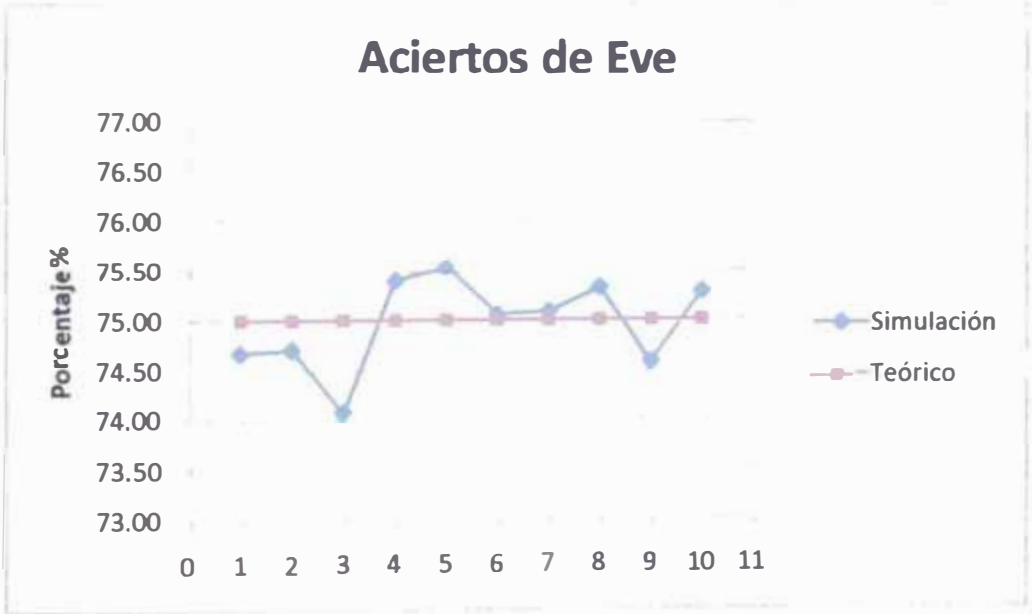


Figura 68: La diferencia máxima entre el valor teórico y la simulación es menos del 1%.

5.5 Simulación de transmisión con un ataque parcial de probabilidad λ sin ruido (Photon Number Splitting)

En este caso el espía interviene aleatoriamente algunos fotones enviados por Alice y reenvía a Bob un fotón con la polarización que midió Este tipo de ataque es conocido como "Photon Number Splitting" (PNS) (37). En el programa se selecciona en la esquina superior izquierda la opción "Con Intruso (PNS)" (Figura 69).

Figura 69: Del ListBox que se encuentra en la esquina superior izquierda se selecciona "Con Intruso (PNS).

Sea el mensaje secreto "Facultad de Ciencias UNI - QKD", tiene 30 caracteres, entonces Alice enviará 48 mil fotones Si Eve ataca por ejemplo sólo el 60% de fotones, el programa obtiene un QBER de 14.75% (la teoría predice 15%, párrafo 4.3, fórmula 65), Bob obtiene un acierto de 85 04% (la teoría predice 85%, párrafo 4.3, fórmula 63) y Eve un acierto de 65.78% (la teoría predice 65%, párrafo 4.3, fórmula 70) (Figura 70).

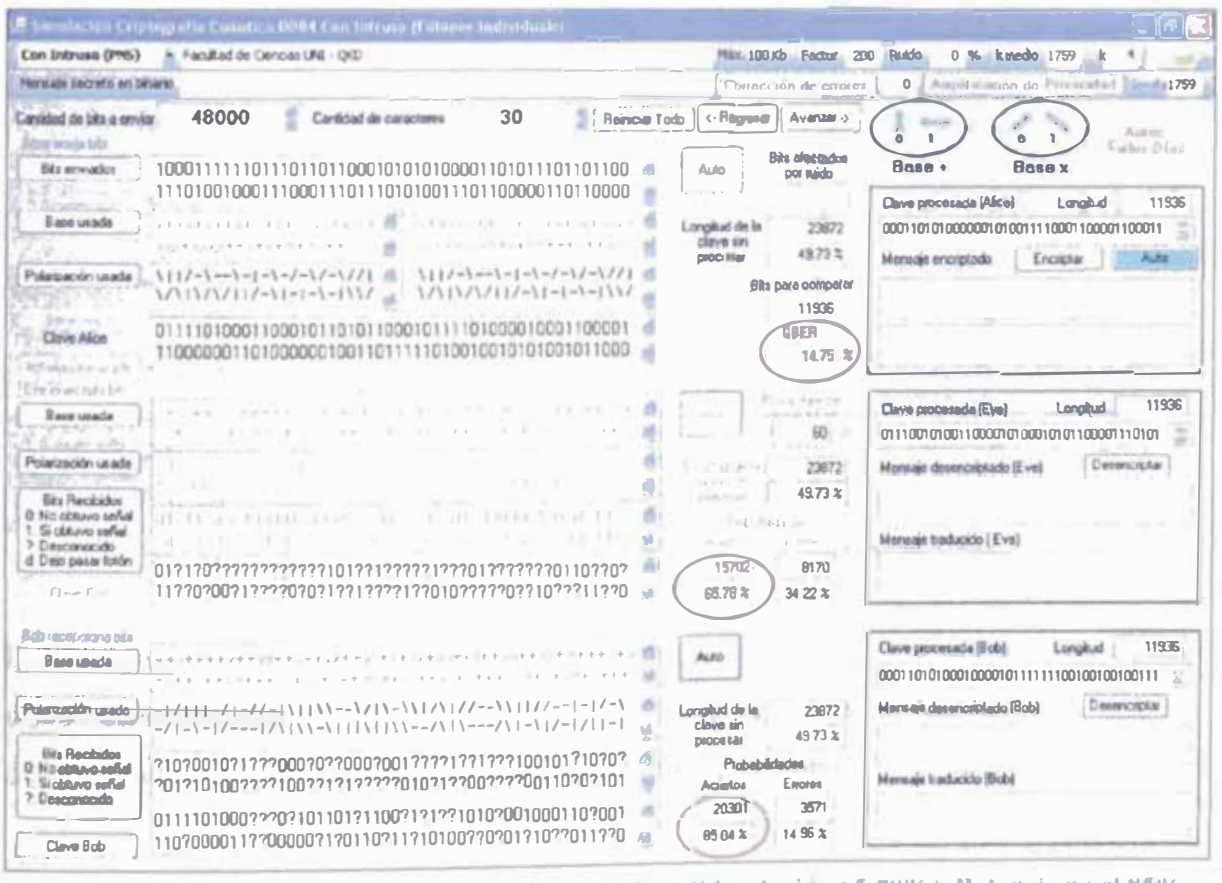


Figura 70: Teóricamente Eve acierta el 65% de la clave (Simulación 65.78%), Bob acierta el 85% (Simulación 85.04%) y el QBER es 15% (Simulación 14.75%).

A pesar de que Eve tiene la probabilidad de acertar el 65% de la clave no significa que tiene el 65% de caracteres correctos, pues un carácter está formado por 8 bits, por tanto si Eve quiere obtener un carácter, tendrá que acertar 8 veces consecutivas de un conjunto de dos posibilidades: 0 ó 1.

La probabilidad de que Eve acierte un carácter es:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 65% = 0.25391%

En la simulación Eve tiene una probabilidad de acertar un carácter de:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 65.78% = 0.25695%

A continuación se corrige el error para ver si Bob puede obtener un mensaje legible. Clic al botón "Corrección de errores" y "Amplificación de Privacidad" (Figura 71).

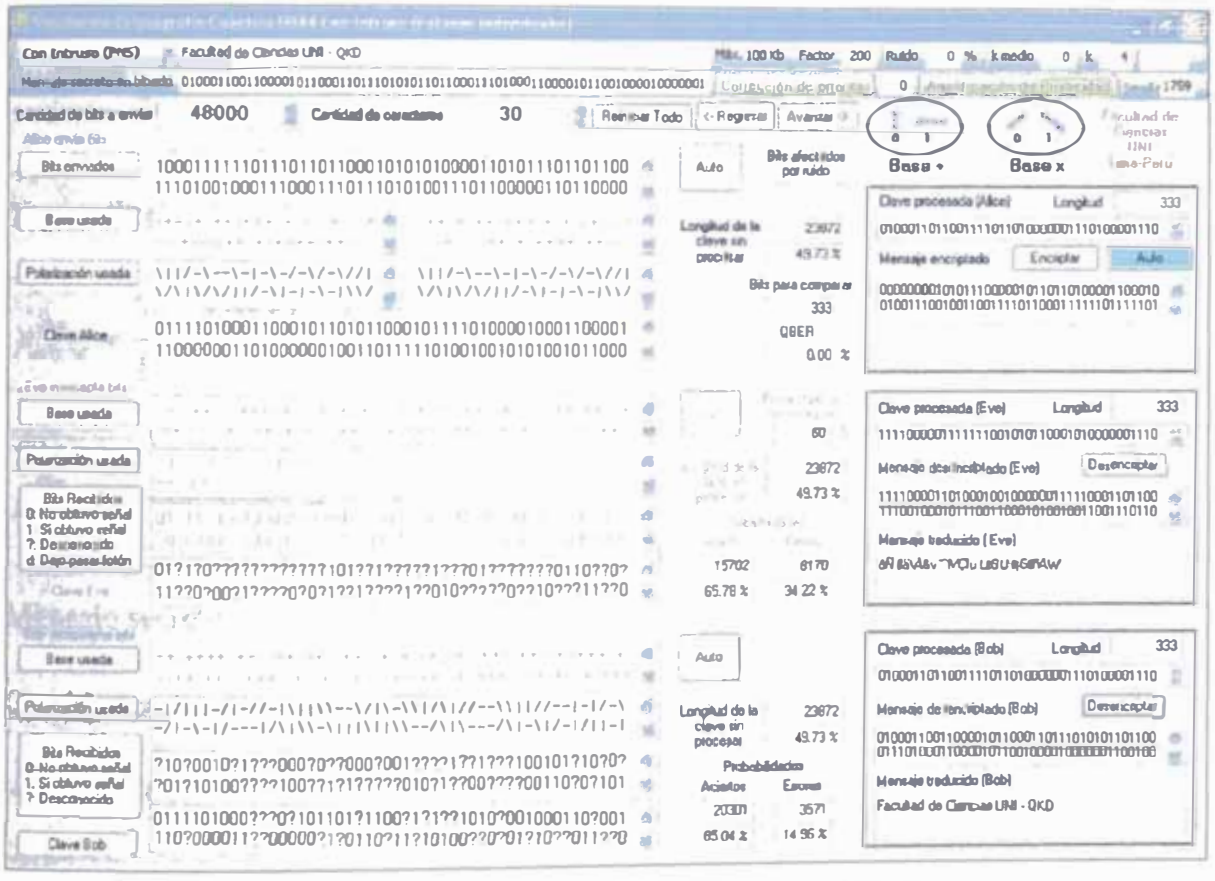


Figura 71: Luego de corregir y amplificar se logra un QBER=0.00%.

Después de la corrección y amplificación el programa logra depurar las claves y obtiene claves idénticas para Alice y Bob sin embargo Eve no puede descubrir la clave y obtiene un mensaje ilegible si es que interviene el mensaje encriptado. Como se

menciono antes, el programa corrige con seguridad hasta un QBER de 20% y con bastante probabilidad entre 20% y 25%.

Gráfica de comparación con el valor teórico

Se ejecuto varias veces el programa, Tabla 6, y se realizó una gráfica para comparar con el valor teórico (Figura 72, 73 y 74).

En el párrafo 4.3, se obtiene para Bob:

$$p_{acertar}^{Bob} = (1-\lambda) + \frac{3}{4}\lambda = 1 - \frac{\lambda}{4}$$

$$p_{equivocar}^{Bob} = \frac{\lambda}{4}$$

$$QBER = \frac{\lambda}{4}$$

Y para Eve:

$$p_{acertar}^{Eve} = \frac{3}{4}\lambda + \frac{(1-\lambda)}{2} = \frac{1}{2} + \frac{\lambda}{4}$$

$$p_{equivocar}^{Eve} = \frac{\lambda}{4} + \frac{(1-\lambda)}{2} = \frac{1}{2} - \frac{\lambda}{4}$$

Mensaje secreto a enviar: Facultad de Ciencias

Cantidad de bits a enviar: 32000

Ataque λ: 60%

Ataque parcial λ=0.60 sin ruido											
Simulación	Lambda	Alice			Bob			QBER %	Eve		
		Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %		Longitud	Porcent. %	Aciertos %
1	0.60	32000	16040	50.13	16040	50.13	84.88	14.96	16040	50.13	64.83
2	0.60	32000	16006	50.02	16006	50.02	85.07	14.92	16006	50.02	65.06
3	0.60	32000	15953	49.85	15953	49.85	84.60	15.58	15953	49.85	65.54

4	0.60	32000	16028	50.09	16028	50.09	85.33	14.56	16028	50.09	65.78
5	0.60	32000	15975	49.92	15975	49.92	84.79	15.11	15975	49.92	64.74
6	0.60	32000	16072	50.23	16072	50.23	85.43	14.60	16072	50.23	65.69
7	0.60	32000	16067	50.21	16067	50.21	85.17	14.60	16067	50.21	65.19
8	0.60	32000	16169	50.53	16169	50.53	84.91	14.63	16169	50.53	65.27
9	0.60	32000	16007	50.02	16007	50.02	84.84	15.03	16007	50.02	65.72
10	0.60	32000	15890	49.66	15890	49.66	84.66	15.44	15890	49.66	64.63

Teórica-mente	Lambda	Alice			Bob			QBER %	Eve		
		Cantidad de bits a enviar	Longitud	Porcent. %	Longitud	Porcent. %	Aciertos %		Longitud	Porcent. %	Aciertos %
1	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
2	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
3	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
4	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
5	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
6	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
7	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
8	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
9	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00
10	0.60	32000	16000	50.00	16000	50.00	85.00	15.00	16000	50.00	65.00

Tabla 6: Datos simulados con un espía parcial (λ=60%) y sin ruido.

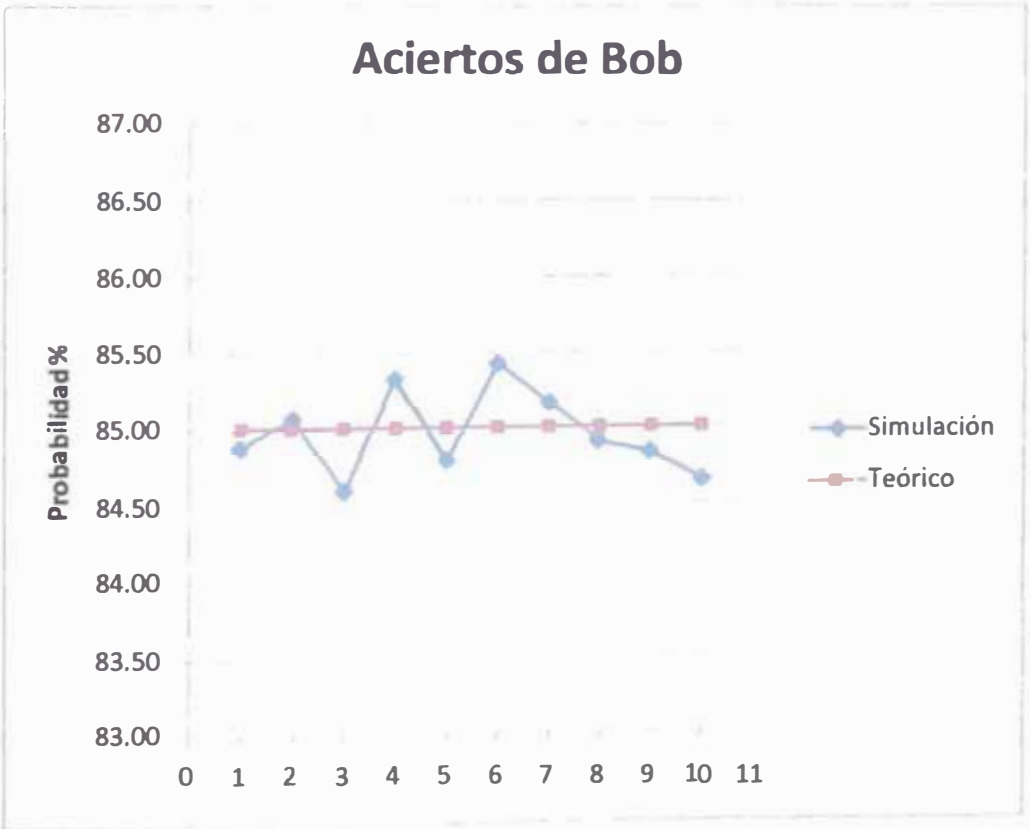


Figura 72: La diferencia máxima entre el valor teórico y la simulación es menos del 0.5%.

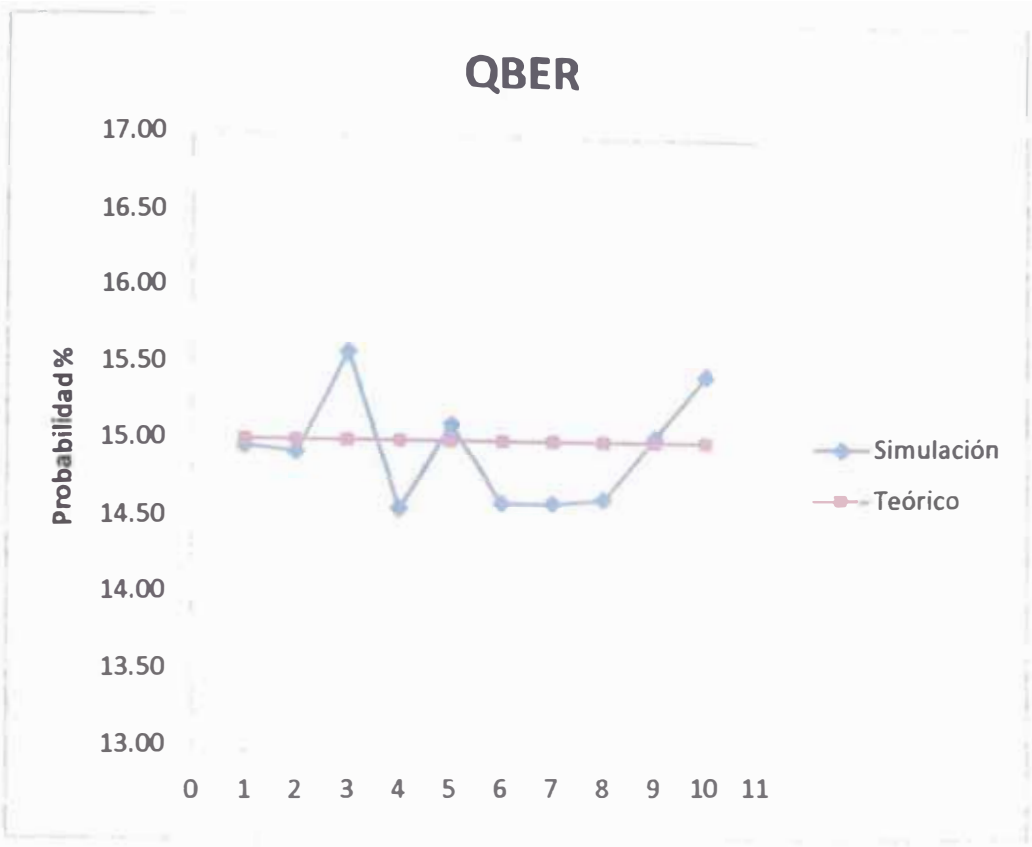


Figura 73: La diferencia máxima entre el valor teorico y simulado es menos del 0.6%.

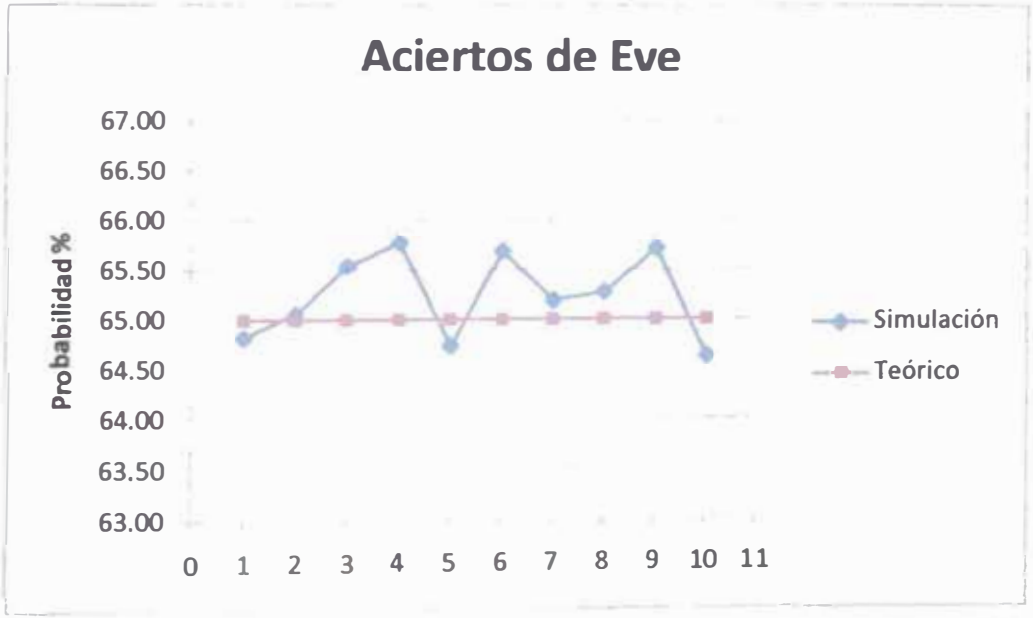


Figura 74: La diferencia máxima entre el valor teórico y simulado es menos del 0.8%.

5.6 Simulación de transmisión con un ruido δ% y ataque parcial de probabilidad λ

Este es el caso extremo donde el fotón puede ser afectado por el ruido y/o por el espía. En el programa se selecciona en la esquina superior izquierda la opción "Con Intruso (PNS)" (Figura 75).

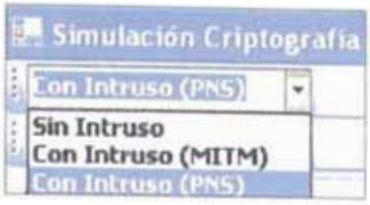


Figura 75: Del ListBox que se encuentra en la esquina superior izquierda se selecciona "Con Intruso (PNS).

Sea el mensaje secreto "Facultad de Ciencias UNI - QKD", tiene 30 caracteres y Alice enviará 48 mil fotones. Por ejemplo, si la transmisión es afectada por un ruido de 20% y Eve ataca solo el 75% de fotones, el programa obtiene un QBER de 26.78% (la teoría predice 27.08%, párrafo 4 5, fórmula 89), Bob obtiene un acierto de 72.93% (la teoría predice 72.92%, párrafo 4 5, fórmula 87) y Eve un acierto de 64.10 (la teoría predice 63.75%, párrafo 4.5, fórmula 98) (Figura 76).

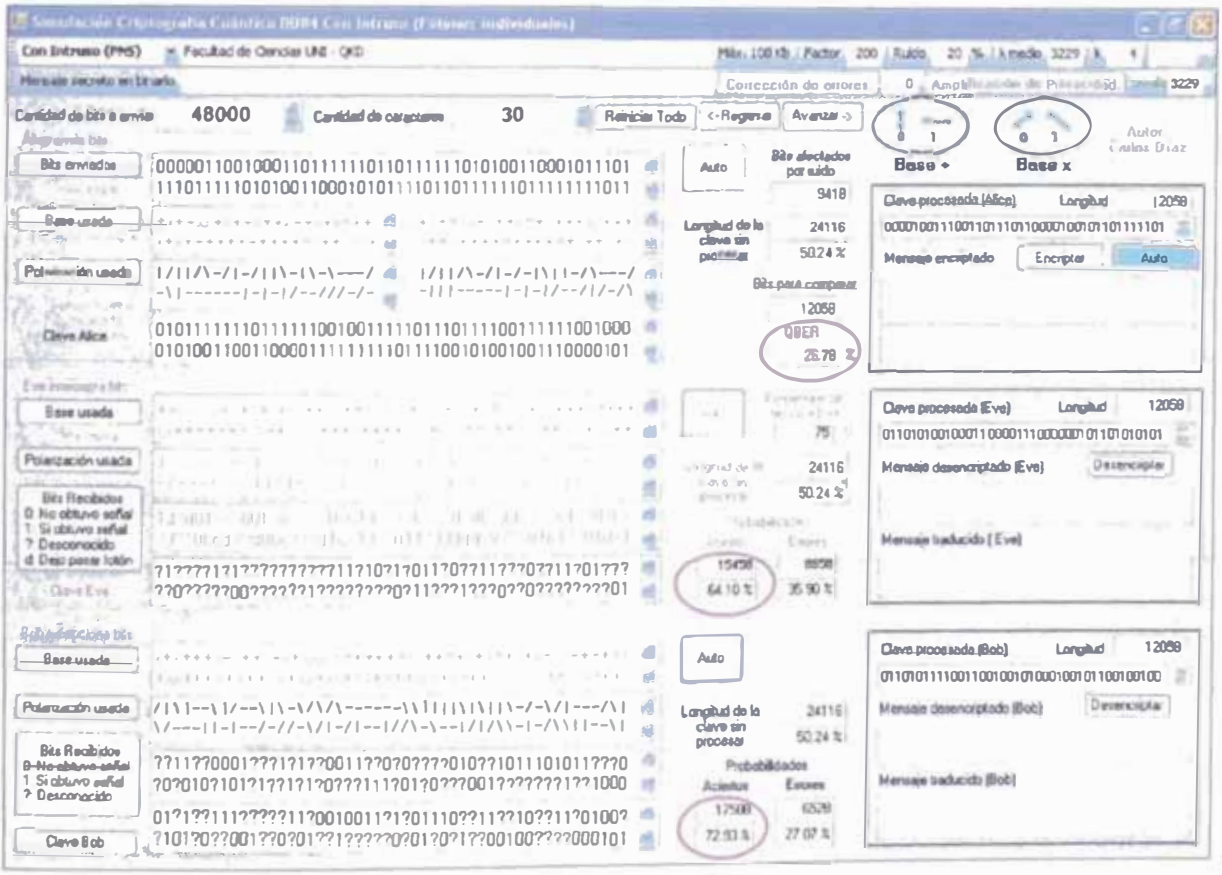


Figura 76: Teóricamente Eve acierta el 63.75% de la clave (Simulación 64.10%), Bob acierta el 72.92% (Simulación 72.93%) y el QBER es 27.08% (Simulación 26.78%).

A pesar de que Eve tiene la probabilidad de acertar el 63 75% de la clave no significa que tiene el 63.75% de caracteres correctos, un carácter está formado por 8 bits, por tanto si Eve quiere obtener un carácter, tendrá que acertar 8 veces consecutivas de un conjunto de dos posibilidades (0 ó 1).

La probabilidad de que Eve acierte un carácter es:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 63.75% = 0.24902%

En esta simulación Eve tiene una probabilidad de acertar un carácter de:

1/2*1/2*1/2*1/2*1/2*1/2*1/2*1/2 de los 64.10% = 0.25039%

Como el QBER es 26.78%, se intenta corregir el error, Bob podría obtener un mensaje legible, clic el botón "Corrección de errores" y "Amplificación de Privacidad" (Figura 77).

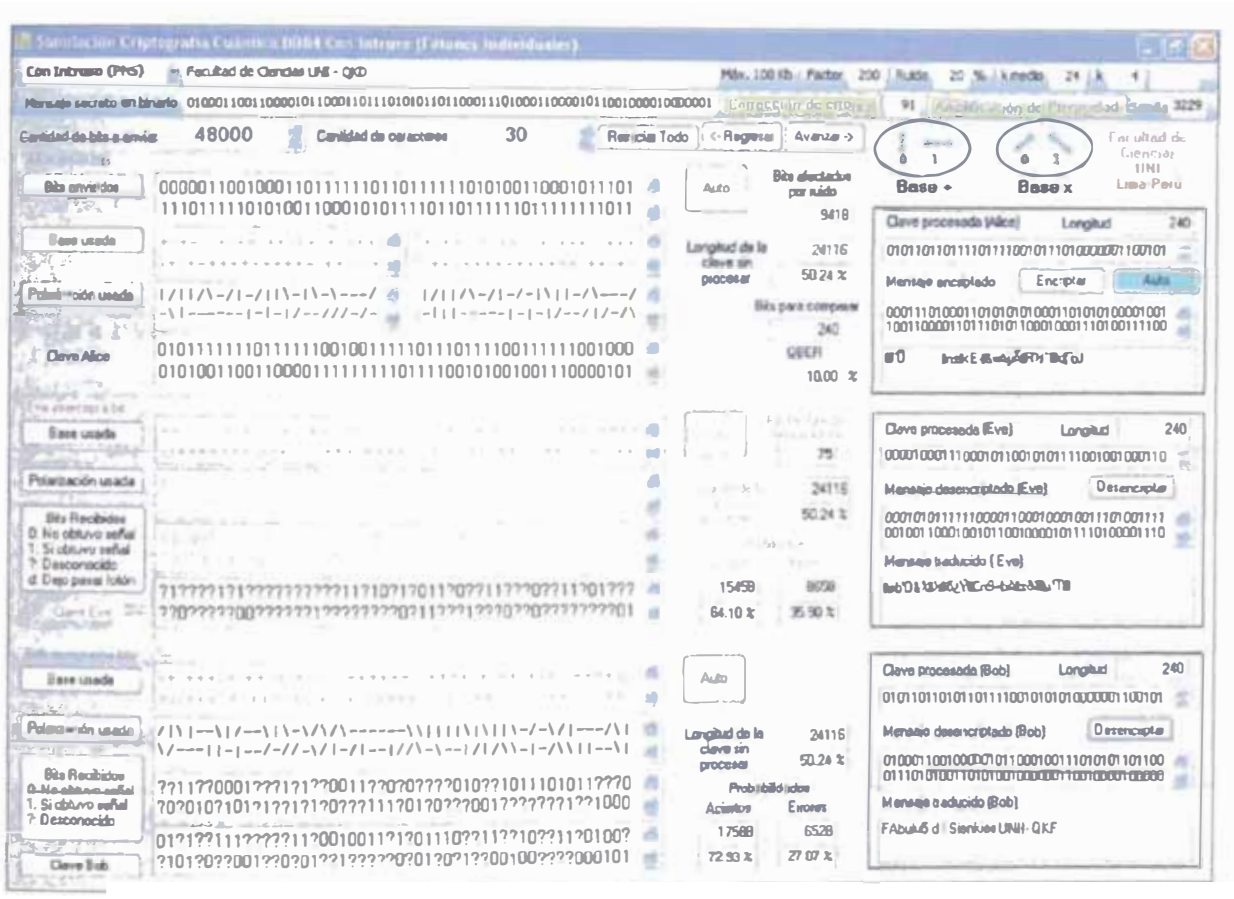


Figura 77: Luego de corregir y amplificar se logra reducir el QBER a 10.00%. Obviamente si Alice envía el mensaje encriptado con ese error, Bob obtendrá un mensaje poco legible. Eve se encontrará en una situación peor.

Vemos que después de la corrección y amplificación el programa no logra depurar las claves y por tanto Alice y Bob obtiene claves distintas, Si Alice envía el mensaje

encriptado, la clave de Bob no podrá desencriptarla correctamente y menos Eve. Sin embargo Bob podría intuir el mensaje que envío Alice. Como mencionamos antes, nuestro programa corrige con seguridad hasta un QBER de 20% y con bastante probabilidad entre 20% y 25%.

Gráfica de comparación con el valor teórico

Se ejecuto varias veces el programa, Tabla 7, y se realizó una gráfica para comparar con el valor teórico (Figura 78, 79 y 80).

En el párrafo 4.5, se obtiene para Bob:

$$p_{acertar}^{Bob} = \left(100 - \frac{2}{3}\delta - 25\lambda + \frac{1}{3}\lambda\delta\right)\%$$

$$p_{equivocar}^{Bob} = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\%$$

$$QBER = \left(25\lambda + \frac{2}{3}\delta - \frac{1}{3}\lambda\delta\right)\%$$

Y para Eve:

$$p_{acertar}^{Eve} = \left(50 + 25\lambda - \frac{1}{3}\lambda\delta\right)\%$$

$$p_{equivocar}^{Eve} = \left(50 - 25\lambda + \frac{1}{3}\lambda\delta\right)\%$$

Mensaje secreto a enviar: Facultad de Ciencias

Cantidad de bits a enviar: 32000

Ataque λ: Varios valores

Ruido δ: Varios valores

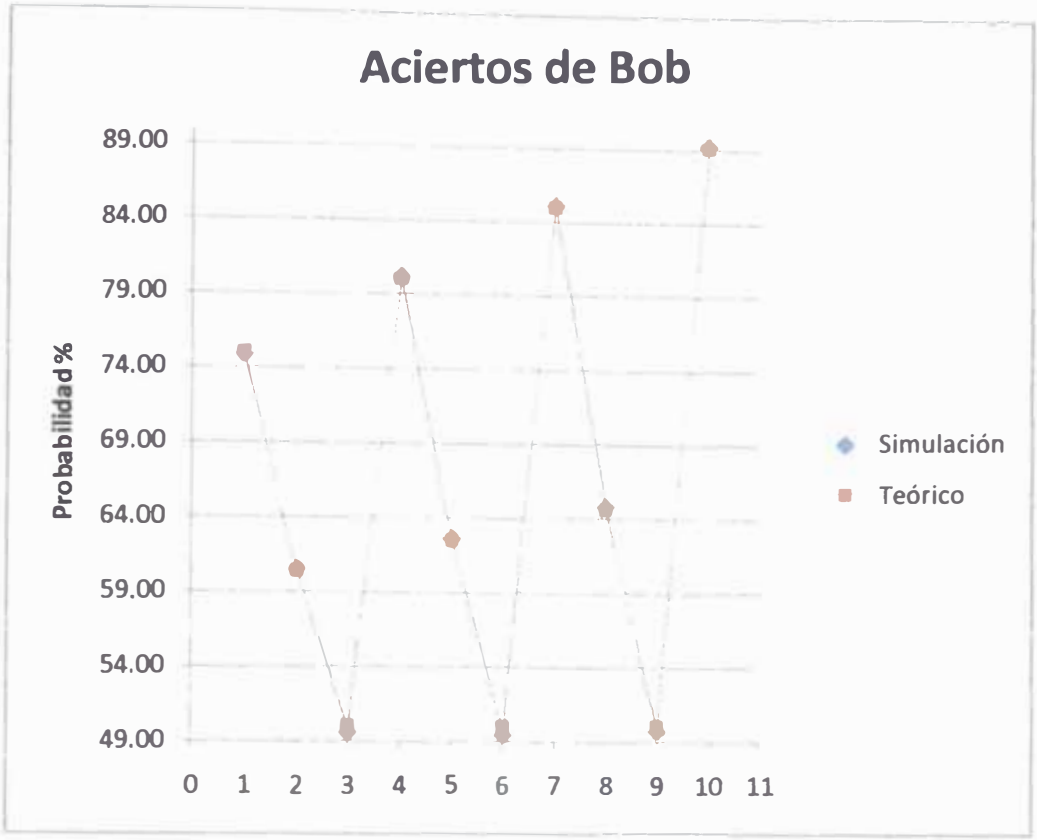


Figura 78: El error absoluto entre el valor teórico y la simulación es menos del 0.6%.

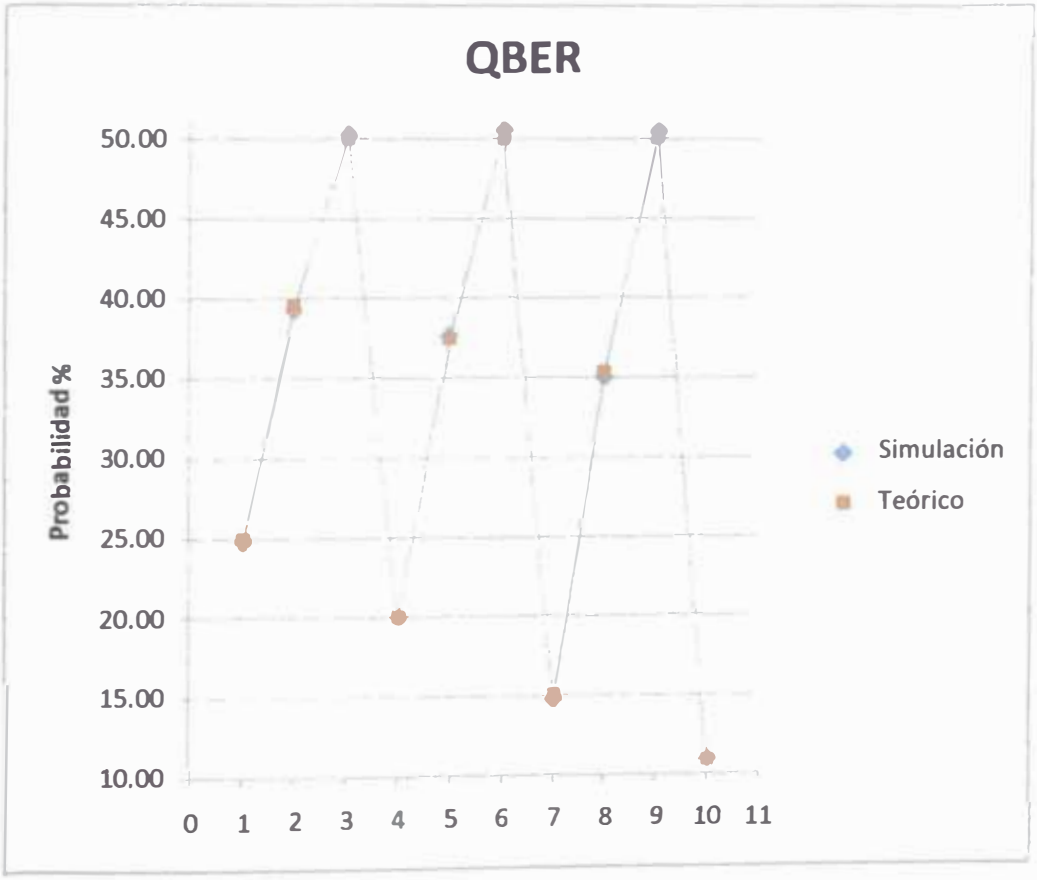


Figura 79: La diferencia máxima entre el valor teórico y simulado es menos del 0.6%.

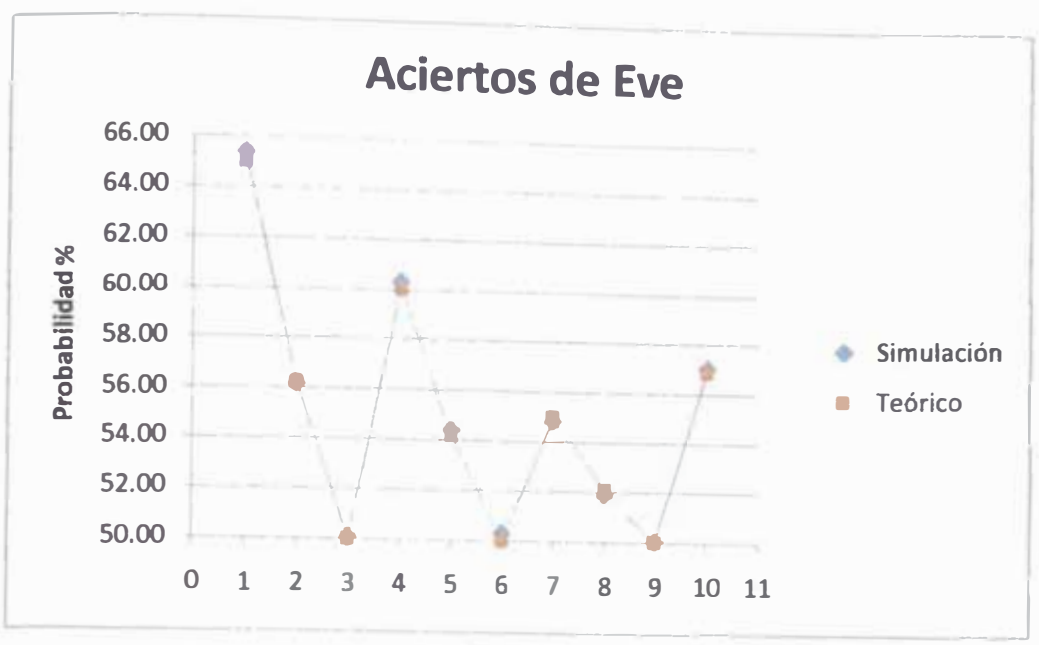


Figura 80: La diferencia máxima entre el valor teórico y simulado es menos del 0.5%.

Como último ejemplo se construye una clave lo suficientemente grande para enviar el Himno de la UNI con un ruido del 10%, se utilizó un Factor 20, es decir 160 bits por carácter lo suficientemente grande para poder realizar la corrección de errores.

HIMNO DE LA UNI

Ingenieros estudiantes
Cantemos nuestra canción
Con el alma bien templada
Y muy alto el corazón.

Seremos para la patria
Lo que nuestros andes son
Peldaños que la agigantan
Y la elevan hacia el sol.

En la ciencias y en las artes mil triunfos
Mil triunfos obtuvimos
Siempre listos estaremos
Para otros mil conquistar.

Ingenieros estudiantes
Cantemos nuestra canción
Con el alma bien templada
Y muy alto el corazón.

La Figura 81 muestra el resultado de la generación de la clave, se obtiene un QBER de 6.58%. Colocando el puntero sobre el área que indica la circunferencia roja aparecerán dos cuadros con los mensajes que hasta el momento tienen Alice y Bob (Figura 82).

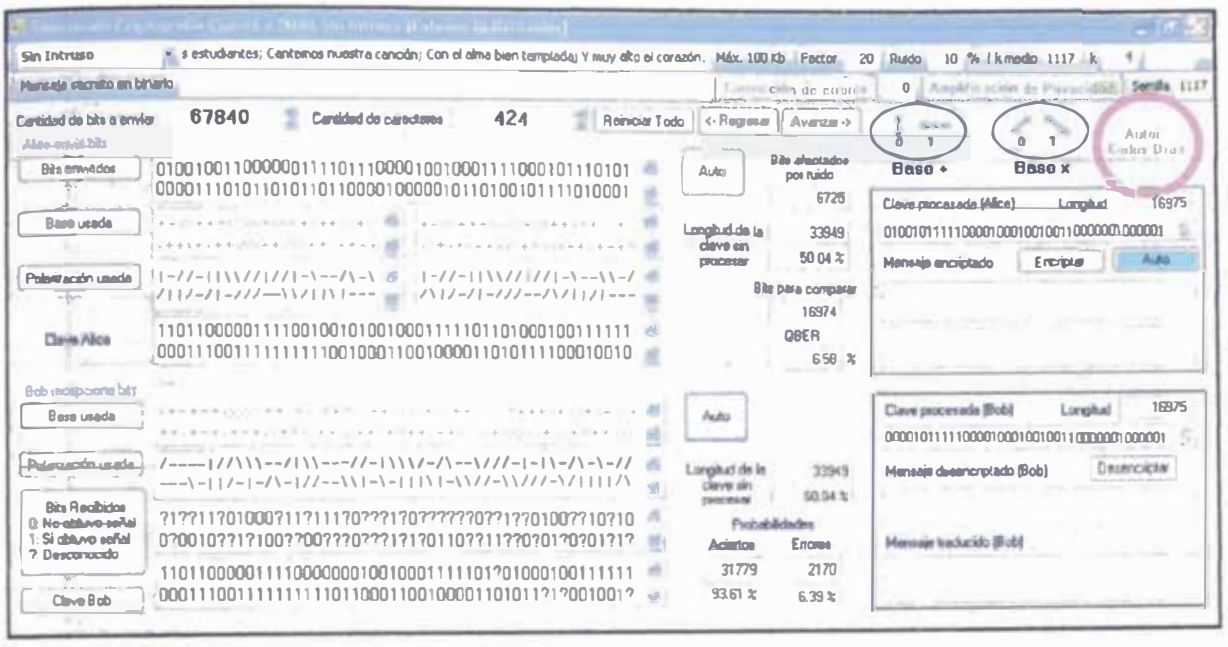


Figura 81: Simulación del envío del Himno de la UNI.

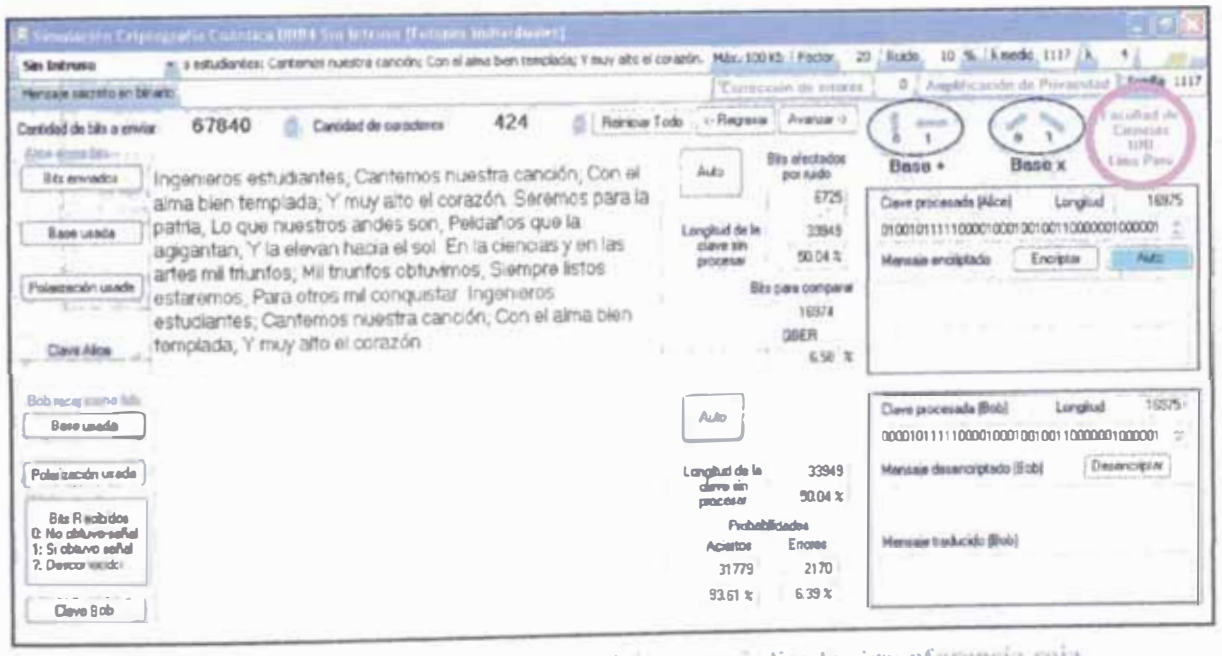


Figura 82: Colocando el puntero sobre el área que indica la circunferencia roja aparecen unos cuadros con los mensajes que tienen hasta el momento Alice y Bob.

Luego de la corrección de errores y amplificación de privacidad, el QBER se reduce a 0.00%. La Figura 83 muestra los resultados, la transmisión se realizó con éxito.

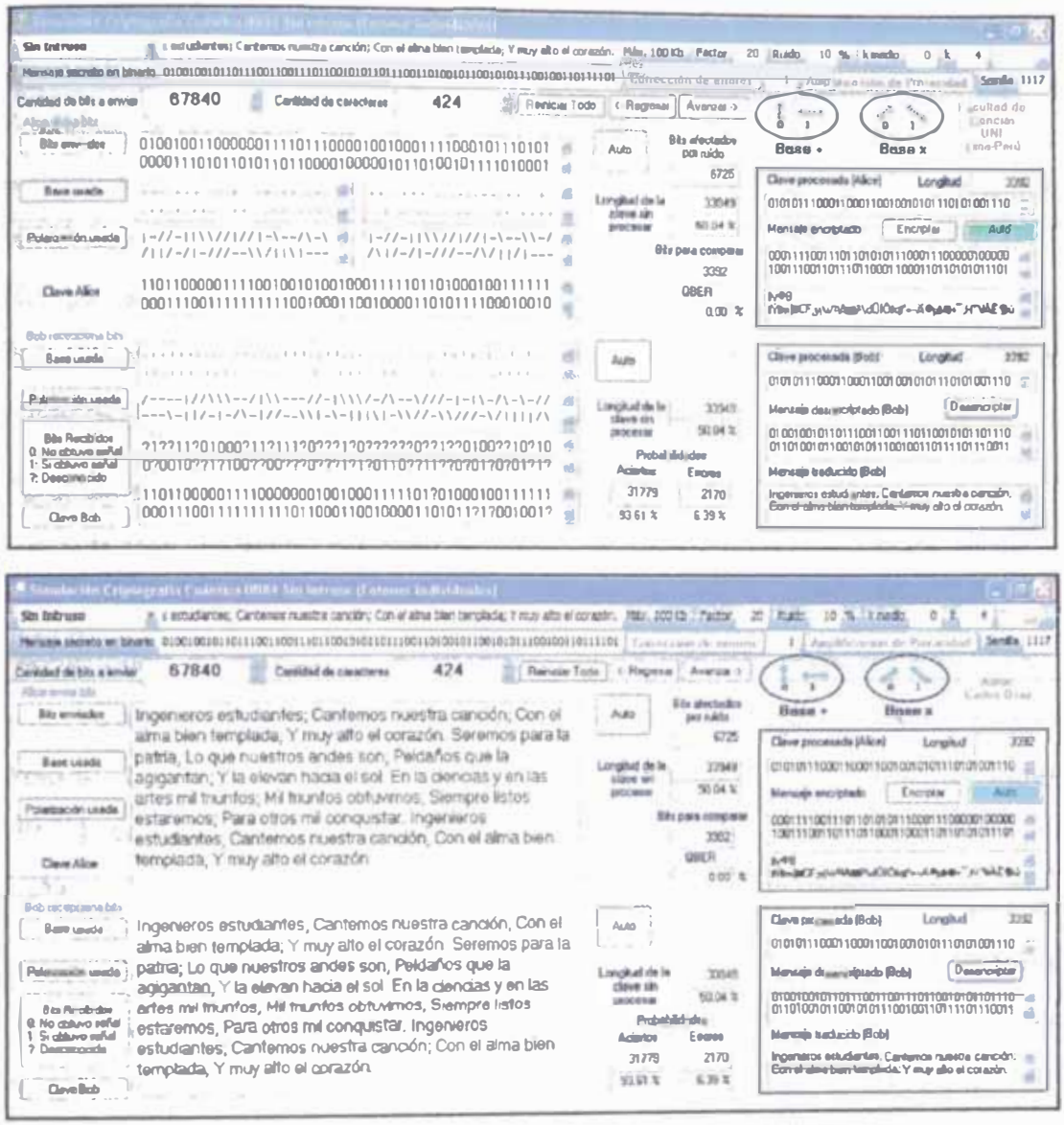


Figura 83: Luego de aplicar la corrección de errores, el QBER se reduce de 6.58% a 0.00%.

5.7 Resumen del proceso de simulación

1. Se ha efectuado simulaciones en computadora clásica de los diversos aspectos del protocolo cuántico BB84, adaptados al diseño de la máquina construida y con la finalidad de comparar con los resultados calculados por las fórmulas teóricas. La ejecución de los programas (cuyos códigos se presentan en el Apéndice D) comprueban los cálculos teóricos dentro de las probabilidades esperadas. Por ejemplo, sin ataque o intervención del espía, el software muestra que la coincidencia de bases es aproximadamente el 50% de la cantidad de bases utilizadas por Alice, como se espera teóricamente (Tabla 2 y Figura 40).

2. También muestra que los métodos de ataque siempre influyen en la formación de la clave de Bob, haciendo posible que Alice y Bob se percaten que han sido espiados. Esto da una idea de la seguridad del protocolo y muestra que Eve tiene una bajísima probabilidad de acertar en la definición de un carácter alfanumérico, obteniendo siempre mensajes ilegibles (0.29% en el método de interceptación "Man in the Middle" (MITM) y un porcentaje similar en el método "Photon Number Splitting" (PNS), en este último caso dependiendo del porcentaje de desvío) (Página 120 y 125).

3. La simulación muestra que es posible trabajar con errores en la transmisión y corregir las claves generadas mediante procesos de criptografía clásica, enviando el mensaje de Alice a Bob sin dificultad. Por ejemplo el programa puede trabajar correctamente a pesar de tener una Tasa de Error de Qubits (QBER) de hasta 20% y con una buena probabilidad hasta 25%.

4. La simulación demuestra que es factible, usando una computadora clásica, simular algunos procesos cuánticos que verifiquen deducciones teóricas.

Capítulo 6

Construcción de una primera Máquina de Criptografía

El equipo que se ha construido es un prototipo básico de un criptógrafo que utiliza el protocolo cuántico BB84 para enviar una clave encriptada por aire libre a una distancia de 1.5 m (Figura 84 y 85).

La máquina construida tiene un diseño de funcionamiento totalmente diferente a las máquinas modernas utilizadas en otras tesis, y fue ideada por nosotros debido a los escasos recursos económicos, sin embargo funciona y demuestra que el protocolo BB84 es eficaz.

Figura 84: Laboratorio donde se construyó y comprobo la maquina de criptografía.

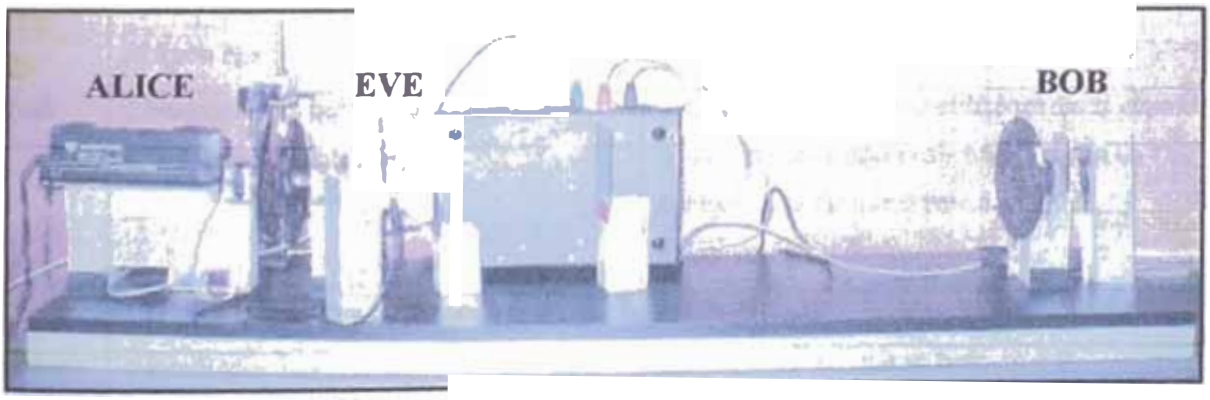


Figura 85: La máquina de criptografía construida, comprueba el protocolo cuantico BB84.

La máquina construida consta de 3 partes. el emisor Alice, el canal cuántico y el receptor Bob. Además se ha incluido un canal de interceptación o del espia Eve para probar la eficiencia de la máquina y se utiliza el portapapeles de Windows como el canal clásico.

En la Tabla 8 se compara una máquina moderna y la construida:

	Máquina moderna	Máquina construida
Alice	4 diodos Láser pulsados, 1 mW. Tiempo por pulso ≤100 ps. Frecuencia de repetición entre 10 kHz y 40 MHz.	1 Láser He-Ne, 1 mW (se simula cuatro láseres usando discos giratorios). Tiempo del pulso determinado por un disco giratorio (1.2 s) *Frecuencia de repetición determinada por discos giratorios* (1/3.9=0.26 Hz)
	Espejo cónico para direccionar el láser.	No tiene.
	Filtros para atenuar el láser.	No tiene. En su lugar se construyó un atenuador manual casero.
	Lente convergente para concentrar el láser.	No tiene.
	Filtro espacial (Pinholes) para asegurar la coherencia espacial antes de salir al canal cuántico.	No tiene
Canal Cuántico	Sistema de lentes convergentes y divergentes para dirigir el láser.	No tiene
	Filtro espacial (Pinholes) para asegurar la coherencia espacial antes de llegar a Bob	No tiene
Bob	Filtro espectral para asegurar la coherencia temporal. Deja pasar sólo la frecuencia de los láseres y rechaza cualquier otra frecuencia espuria.	No tiene
	1 beamsplitter no polarizador para ofrecer al fotón dos caminos a seguir.	No tiene
	2 beamsplitters polarizadores para analizar la polarización del fotón.	No tiene. En su lugar se utilizó un disco giratorio con cuatro polarizadores y un programa de computadora de apoyo para analizar la polarización del fotón.
	1 lámina retardadora media onda	No tiene
	4 fotodiodos de avalancha de Silicio para detectar fotones.	No tiene. En su lugar se tiene un solo fototransistor.

Tabla 8: Cuadro comparativo entre una máquina convencional y la máquina construida.

Eve es un espía que tecnológicamente se espera tenga iguales o mejores equipos que Alice y Bob (Tabla 8) Por tanto posee elementos (tipo beamsplitters) para desviar parte de los fotones, detectarlos y volver a generarlos. En nuestro caso, por los limitados

recursos económicos, Eve utiliza, en lugar de beamsplitters, dos vidrios comunes y como detectores de fotones, solo dos polarizadores fijos y dos fototransistores.

Como el prototipo construido envía pulsos de fotones, el fenómeno se puede explicar también en términos de la óptica clásica. Aquí es importante mencionar que solo cuando se logre enviar y detectar fotones individuales[54] el efecto cuántico será el que predomine y muestre las ventajas en seguridad de este sistema, tal como lo predice la Mecánica Cuántica.

También por las limitaciones antes mencionadas se ha utilizado una electromecánica lenta que solo permite enviar un pulso cada 3 9 segundos. Esto trae como resultado que si se desea crear una clave para 6 caracteres (96 bits)[55] el proceso demorará 6.24 minutos. A pesar de esta dificultad el equipo construido permite demostrar el funcionamiento básico de un criptógrafo cuántico Se podría decir que se muestra este proceso en "cámara lenta".

Es importante mencionar que debido a estas limitaciones solo es posible generar la llave secreta en bruto (raw key). Las etapas de reconciliación de información (corrección de errores) y de amplificación de privacidad requieren de un gran número de bits transmitidos en tiempos razonables

Las partes opto-electro-mecánico de este equipo funcionan sincronizadamente.

- Los elementos ópticos están constituidos por un laser He-Ne, polarizadores, fototransistores y vidrios.
- La parte electro-mecánica está constituido por motores a paso, discos e interface electrónica con conexión paralela a la PC.
- El software de control consistente de tres programas independientes, implementan el protocolo cuántico BB84 y sincroniza el envío y detección de los pulsos láser.

[54] Actualmente no existen fuentes sincronizadas que envíen un solo fotón cada vez que se le pida. En su lugar se suele utilizar pulsos laser atenuados cuya energía se ha absorbido tanto que estadísticamente se puede afirmar que tiene un solo fotón o también se utiliza fotones generados por una fuente de Conversión Paramétrica Espontanea Descendente (Spontaneus Parametric Down Conversion) (51). Sin embargo las investigaciones con puntos cuánticos (Quantum Dots) hace suponer que en poco tiempo se tengan emisores sincronizados de fotones totalmente funcionales.

[55] Cada carácter necesita 8 bits para ser encriptado, como el protocolo BB84 crea una clave que está formada probabilísticamente por el 50% de la señal enviada por Alice entonces se necesita 16 bits por carácter.

6.1 Configuraciones experimentales utilizadas

En la prueba de la máquina de criptografía se realizó tres experimentos:

- Distribución de la clave sin espía.
- Distribución de la clave con espía.
- Envío de un mensaje de Alice a Bob.

6.1.1 Distribución de la clave sin espía y sin ruido

En la Figura 86 se muestra el diseño para distribuir las claves utilizando el protocolo cuántico BB84

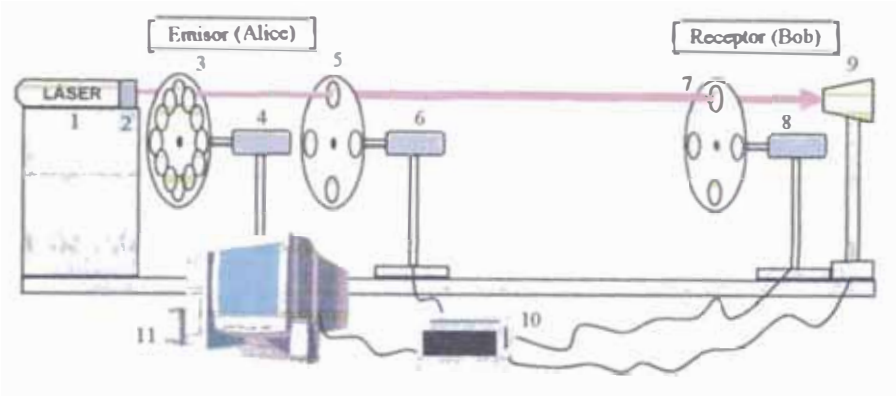


Figura 86: Configuración del equipo sin espía.

1. Un láser continúo de Helio-Neón, 633 nm, 1 mW, polarizado linealmente y utilizado por el emisor (Alice) para enviar la señal al receptor (Bob)
2. Un atenuador manual casero colocado a la salida del láser, construido con un polarizador introducido en un soporte que permite rotarlo. Alice lo utiliza para reducir controladamente la potencia del pulso enviado.
3. Un disco giratorio con 16 aberturas igualmente espaciadas que actúa como chopper. Lo utiliza Alice para producir una secuencia periódica de pulsos.
4. Un motor a paso que gira el chopper.
5. Un disco discos con 4 polarizadores igualmente espaciados que utiliza Alice para enviar pulsos láser con las polarizaciones elegidas aleatoriamente.
6. Un motor a paso que gira el disco de Alice.

7. Un disco con 4 polarizadores igualmente espaciados que utiliza Bob para medir la polarización del pulso que recibe
8. Un motor a paso que gira el disco de Bob.
9. Un fototransistor que Bob utiliza para detectar el pulso incidente.
10. Interface electrónica de control: Tienes dos funciones, una que recibe órdenes de la computadora para girar los motores y otra que envía las medidas del fototransistor a la computadora.
11. Es la parte lógica del equipo y se encarga de implementar el protocolo BB84 así como controlar la interfaz electrónica.

Funcionamiento del software de control para Alice y Bob

Estos programas son independientes y se pueden separar fácilmente en dos computadoras.

- **Programa de Alice**: Lee la cantidad de caracteres que tendrá el mensaje secreto y genera aleatoriamente las bases y polarizaciones necesarias para producir la clave. Luego controla el disco polarizador y el chopper para enviar las polarizaciones a Bob vía el **canal cuántico** que es el aire entre ellos. Al terminar de enviar los pulsos utiliza el portapapeles como **canal clásico** para avisar a Bob que termino de enviar los pulsos. Luego envía las bases que utilizó al portapapeles y compara con las bases que Bob uso para medir (Bob ha publicado estas bases en el portapapeles), con esta información construye su clave, encripta el mensaje y envía el mensaje encriptado al portapapeles
- **Programa de Bob**: Genera aleatoriamente las bases y polarizaciones para medir las polarizaciones de los pulsos enviados por Alice. Controla el disco polarizador para alinear según la polarización elegida, detecta la señal que llega al fototransistor y las almacena para un posterior análisis. Mientras tanto, el programa siempre está observando al portapapeles y cuando encuentra el aviso de que Alice termino de enviar entonces detiene la medición y envía al portapapeles las bases que utilizó. Inmediatamente después recupera del portapapeles las bases utilizadas por Alice y compara con sus bases para formar la clave de encriptación. También recupera el mensaje encriptado por Alice y finalmente desencripta el mensaje.

Detalles técnicos para la distribución de la clave sin espía

a) ¿Qué medios se están utilizando como canal cuántico y canal clásico?

El canal cuántico es simplemente el aire entre Alice y Bob. El canal clásico es el portapapeles de Windows

b) ¿Cómo sabe Bob que se inicio el envió de señales?

Al principio Bob está en espera con sus instrumentos encendidos. Alice envía un primer pulso láser que le anuncia a Bob que se va a iniciar la transmisión en 25 ms, entonces a partir del segundo bit ya se consideran las señales validas.

c) ¿Cómo se sincroniza las medidas de Bob con los envíos de pulsos de Alice?

Experimentalmente el tiempo máximo de giro para obtener[56] y confirmar[57] una polarización es 2.7 segundos (esto corresponde a 270°). Naturalmente será menos si gira 90° ó 180°. Una vez que los polarizadores de Alice y Bob están alineados, el chopper gira para dejar pasar el pulso laser vía el canal cuántico, este giro se obtiene y se confirma en 1.2 segundos. Entonces, para sincronizar, el programa mantiene apagado el detector de Bob durante 2.7 segundos y luego se enciende durante 1 2 segundos y después se vuelve a apagar y así continua hasta terminar el envío de las señales. En total el periodo de las medidas es 3.9 segundos.

d) ¿Cómo sabe Bob cuando se detuvo la transmisión?

Bob siempre está mirando el canal clásico (el portapapeles), cuando Alice termina envía un mensaje al portapapeles, Bob lo lee y detiene sus equipos.

e) ¿Cómo construyen Alice y Bob sus claves?

Usan el mismo procedimiento utilizado por el programa de simulación, párrafo 5.2. Es decir que sólo utilizan las bases en las que ambos coincidieron, para saber que bases usaron, ambos lo publican en el portapapeles. Tanto Alice y Bob siempre miran el portapapeles.

[56] Obtener significa que físicamente el disco se encuentra en la posición deseada.
[57] Confirmar significa que el programa ya sabe que está en la posición deseada, obviamente entre obtener y confirmar hay un retraso de tiempo que depende de la velocidad de procesamiento de la computadora, en nuestro caso es del orden de centésimas de segundos.

e) ¿Cómo es enviado a Bob el mensaje encriptado?

Una vez que Alice construyó su clave envía el mensaje encriptado al portapapeles. El mensaje se encripta aplicando el operador XOR al texto en claro en binario y a la clave. Como Bob siempre está pendiente del portapapeles, lo recupera y lo desencripta usando su clave y el operador XOR.

6.1.2 Distribución de la clave con espía (Photon Number Splitting) y sin ruido

Lo correcto es que el espía intervenga con un beamsplitter, pero motivos económicos se tuvo que utilizar vidrios comunes. El diseño se muestra en la Figura 87.

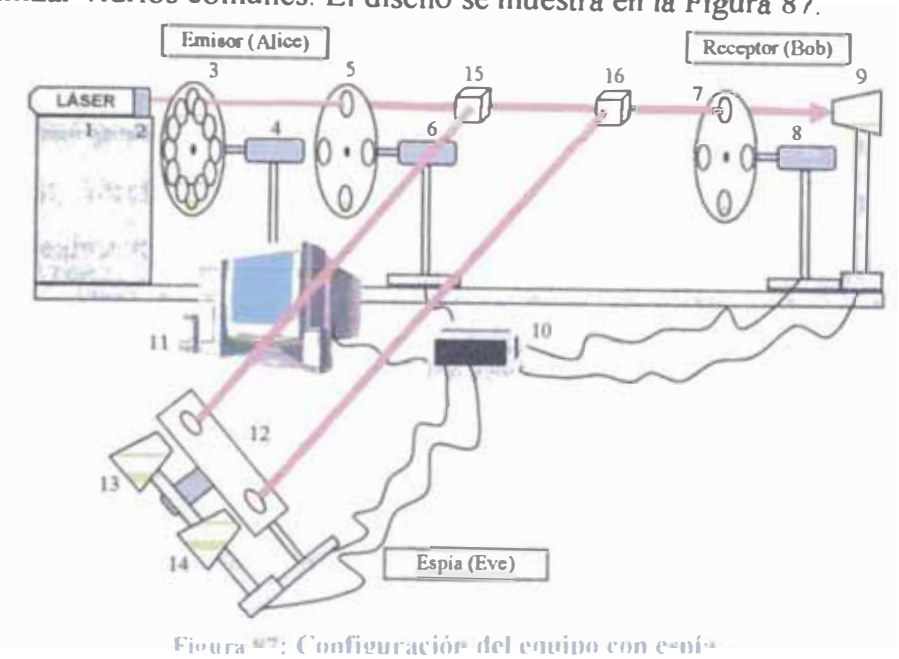


Figura 87: Configuración del equipo con espía

Los ítems desde 1 al 11 son los mismos utilizados para la distribución sin espía ni ruido.

12. Un soporte fijo con 2 polarizadores. Los usa Eve para medir las polarizaciones desviadas por los vidrios ("beamsplitters caseros").

13. Primer fototransistor de Eve. Mide en la base rectilínea +.

14. Segundo fototransistor de Eve. Mide en la base diagonal ×.

15. Un vidrio delgado que funciona como un "beamsplitter casero" que transmite y refleja el pulso láser Lo utiliza el intruso Eve para desviar parte del pulso de fotones enviados por Alice.

16. Otro vidrio que cumple la misma función anterior.

Funcionamiento del software de control para Eve

- **Programa de Eve**: Mide las polarizaciones reflejadas en los vidrios. El programa siempre observa el portapapeles y en cuanto encuentra el aviso que Alice terminó entonces recupera del portapapeles las bases de Alice y Bob y construye su clave de encriptación usando las bases coincidentes entre Alice y Bob. Finalmente Eve utiliza esta clave para desencriptar el mensaje. Los detalles de cómo deduce y construye la clave se encuentran más adelante en el párrafo 7.2.

Detalles técnicos para la distribución de la clave con espía (método PNS)

a) ¿Cómo funciona el atenuador casero?

El atenuador está compuesto por un repuesto de caño de forma tubular que encaja con la salida del laser. Dentro de este repuesto se coloco un polarizador Como el laser es polarizado linealmente entonces girando el repuesto se puede controlar la potencia e intensidad[58] de salida. La tarea del atenuador es disminuir la intensidad del pulso laser, según la ley de Malus, para una onda electromagnética, $I = I_0 \cos^2 \alpha$, donde I es la intensidad del laser que se obtiene a la salida del atenuador, I_0 es la intensidad de entrada al atenuador y α es el ángulo formado por el polarizador Para un fotón el atenuador da preferencia al colapso en una dirección $|\updownarrow\rangle = sin^2 \alpha |\leftrightarrow\rangle + \cos^2 \alpha |\updownarrow\rangle$ cada fotón sale con la misma intensidad de entrada, pero cambiando el ángulo se puede lograr que salgan menos fotones con la polarización inicial $|\updownarrow\rangle$ y así reducir la intensidad total de salida.

b) ¿Cómo influyen los vidrios comunes en la polarización del pulso enviado por Alice?

La luz que se refleja y refracta sobre el vidrio transparente, sufre un cambio en su polarización.

Para cierto ángulo de incidencia, llamado angulo de Brewster, la luz reflejada esta 100% polarizada en dirección perpendicular al plano de incidencia, en cambio la luz refractada

[58] La intensidad es la cantidad de energía por unidad de área y unidad de tiempo.

apenas alcanza un 15% de polarización perpendicular (38), por ejemplo para el caso del vidrio común n = 1.5, el ángulo de Brewster es de 56.31°.

Sin embargo a medida que se reduce este ángulo, los cambios en la polarización también disminuyen, experimentalmente se selecciono un ángulo de aproximadamente 15° donde este cambio no influyo en las medidas esperadas. En el apéndice C se muestra los cálculos

El reflejo del primer vidrio para Eve no influye en las polarizaciones ↕ o ↔, pero para la polarización ⤢ se produjo un cambio del 6% con preferencia a la orientación vertical. Para la polarización ⤡ se produjo un cambio del 6% con preferencia a la orientación vertical.

El reflejo del segundo vidrio para Eve no influye en las polarizaciones ↕ o ↔, pero para la polarización ⤢ se produjo un cambio del 5.3% con preferencia a la orientación vertical. Para la polarización ⤡ se produjo un cambio del 5.3% con preferencia a la orientación vertical.

Para que el pulso llegue a Bob debe pasar por los dos vidrios, es decir que sufre dos refracciones, no influye en las polarizaciones ↕ o ↔, pero para las polarización ⤢ se produjo un cambio del 1.1% con preferencia a la orientación horizontal. Para la polarización ⤡ se produjo un cambio del 1.1% con preferencia a la orientación horizontal.

Capítulo 7

Resultados experimentales

En este Capítulo se comprueba que el protocolo cuántico BB84 funciona correctamente en nuestra máquina. La máquina construida en esta tesis es un diseño simplificado, donde muchos de sus componentes fueron reemplazados por elementos más sencillos debido a los limitados recursos económicos (ver Tabla 8 en el Capítulo 6). Sin embargo los resultados, en lo esencial coinciden totalmente con los esperados en una máquina más sofisticada.

Se realizó tres experimentos.

- **Distribución de la clave sin espía**: En este caso se generó una clave para enviar el mensaje "UNI". El mensaje tiene 24 bits y se utilizó 48 pulsos láser. El tiempo empleado en la distribución de la clave y envío del mensaje fue de 187500 ms = 3 125 minutos. En todas las repeticiones del experimento se logro el éxito esperado.

- **Distribución de la clave con espía**: Se envío el mismo mensaje anterior, empleando la misma cantidad de pulsos y tiempo. En este experimento aparece el espía Eve con dos "beamsplitters caseros" (vidrios comunes). Como se envía pulsos de fotones entonces Eve puede desviar algunos fotones y deducir también la clave, tal como se esperaba. La única forma de lograr que Eve no tenga éxito es atenuando el láser y enviar cada vez menos fotones Debido a que los equipos de Eve son precarios, con la suficiente atenuación se logro evitar que Eve obtenga la clave sin afectar la igualdad de las claves obtenidas por Alice y Bob. Esto demuestra que a medida que se tenga menos fotones por pulso la seguridad aumenta, en el límite, caso cuántico, cada pulso contiene un solo fotón.

- **Envío del mensaje de Alice a Bob**: Este es un experimento adicional que muestra la versatilidad de la máquina construida, que además de distribuir una clave, también se puede usar para enviar el mensaje encriptado.

7.1 Distribución de la clave sin espía

Procedimiento:

1. El programa de Alice lanza un pulso láser a Bob indicándole que iniciará el envió de la clave, esta primera señal no es tomada en cuenta para la clave.

2. El programa, de forma aleatoria selecciona las polarizaciones de Alice y Bob. Luego la interface de control hace rotar los discos hasta obtener las polarizaciones elegidas. El software almacena esta información en una base de datos.

3. Para cada pulso a ser enviado:

   a) El programa de Alice activa el chopper y deja pasar un pulso laser con la polarización elegida.

   b) El programa de Bob, con una polarización aleatoria, detecta con el fototransistor el pulso que llega y almacena la medida en una base de datos.

4. Repite hasta terminar con la cantidad de bits requeridos. Alice comunica a Bob que terminó de enviar la clave vía el canal clásico (portapapeles).

5. Finalmente el software calcula la clave, de forma similar como lo hace en programa de simulación.

Descripción del aparato experimental:

Emisor Alice: Está formado por el laser, el atenuador, el chopper, un disco giratorio con cuatro polarizadores para codificar la información y dos motores a paso (Figura 88).

Figura 88: El emisor Alice.

Receptor Bob: Está formado por un disco giratorio con cuatro polarizadores para decodificar, un motor a paso y un fototransistor (Figura 89).

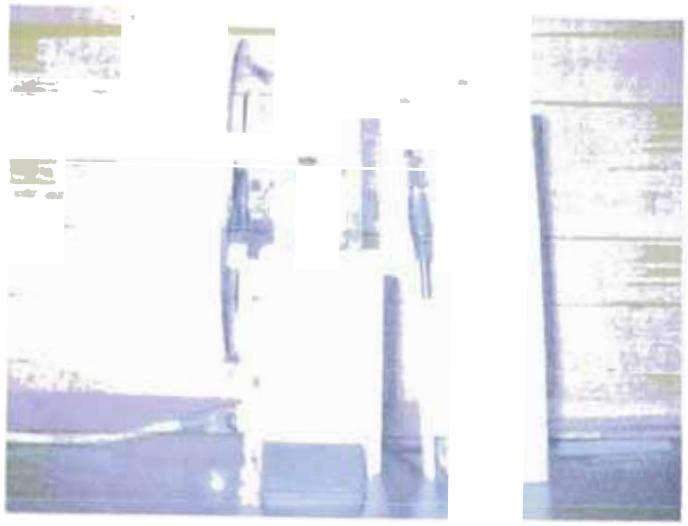
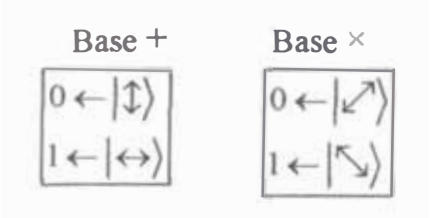


Figura 89: El receptor Bob.

Resultados del experimento:

Para la demostración y explicación se distribuirá una clave de 24 bits, suficientes para luego enviar un mensaje de 3 caracteres.

Se usará la siguiente convención para reconocer cada bit en cada base:



1. Se ejecutan los programas Alice.exe y Bob.exe. Se presiona el botón "Inicio" de Bob que activa su fototransistor y así detectar la señal de inicio del envió de pulsos de fotones En el formulario de Alice se escribe en el cuadro de texto "Mensaje secreto a enviar", el mensaje que se desea enviar a Bob. Esto sirve para que el programa calcule cuantos bits se necesita para construir la clave. El protocolo BB84 se utiliza para construir la clave de encriptación y no para enviar el mensaje.

   Por ejemplo, para enviar la palabra "UNI" (3 caracteres, 24 bits) se necesitarán 48 bits (Figura 90).

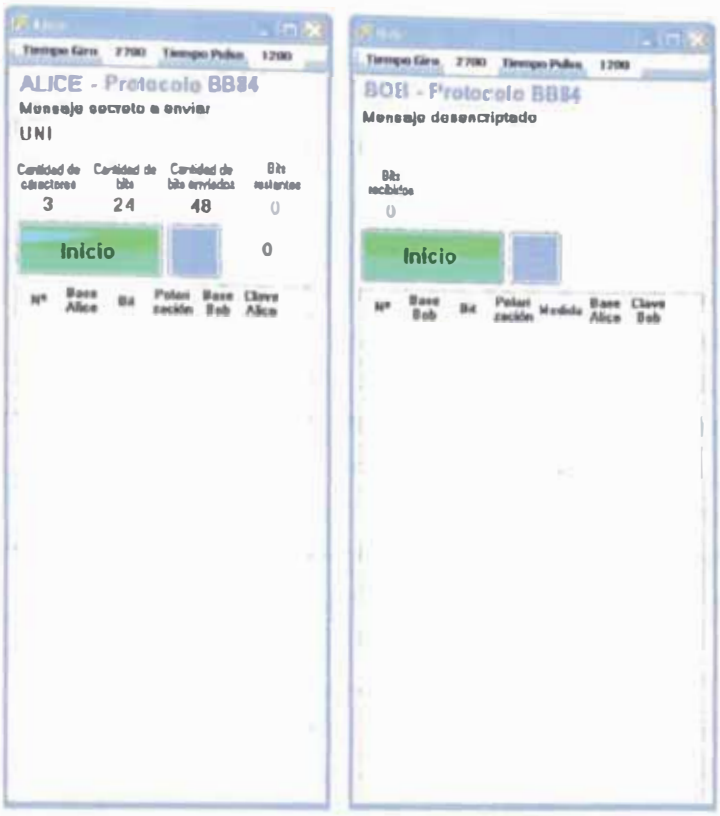


Figura 90: Formularios de Alice y Bob. Alice calcula que serán necesarios 48 bits.

2. Clic al botón "Inicio" de Alice para iniciar la transmisión.

   En la Figura 91 se observa como Alice envía los bits aleatorios en una base aleatoria con la polarización adecuada. Y Bob recepciona los fotones en una base aleatoria con una polarización aleatoria. Bob anota las medidas de su fototransistor. Si detecto anota "1" y si no anota "0".

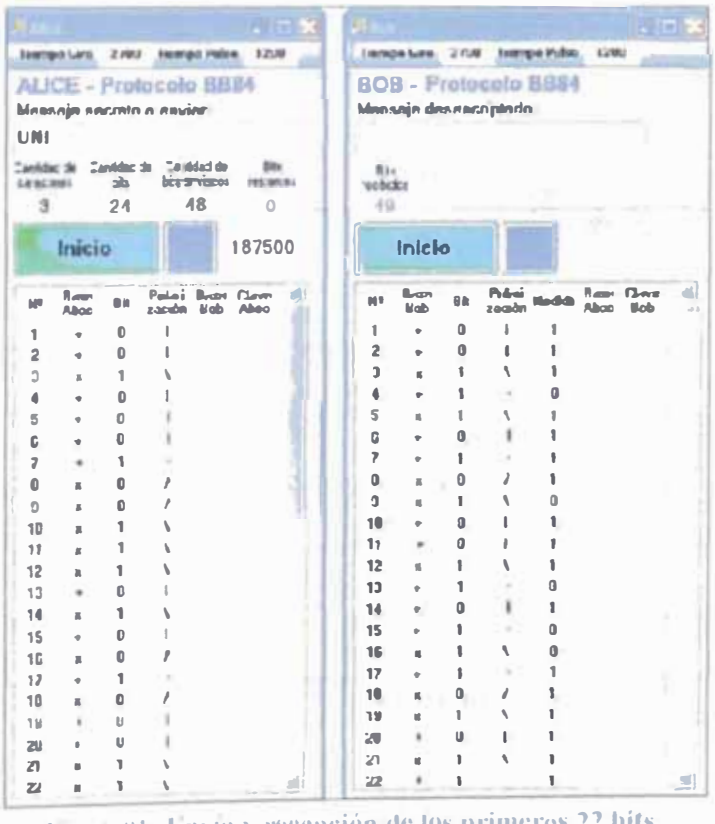


Figura 91: Envío y recepción de los primeros 22 bits.

3. Una vez que terminan publican sus bases vía un canal clásico (portapapeles) (Figura 92).

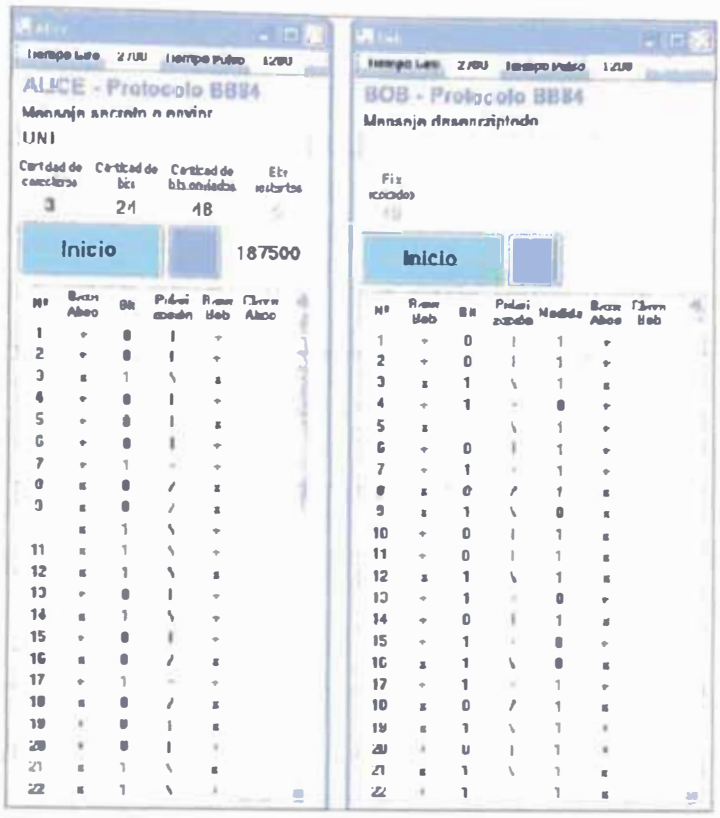


Figura 92: Alice y Bob publican sus bases.

4. Alice y Bob forman sus claves seleccionando las polarizaciones utilizadas de las bases coincidentes.

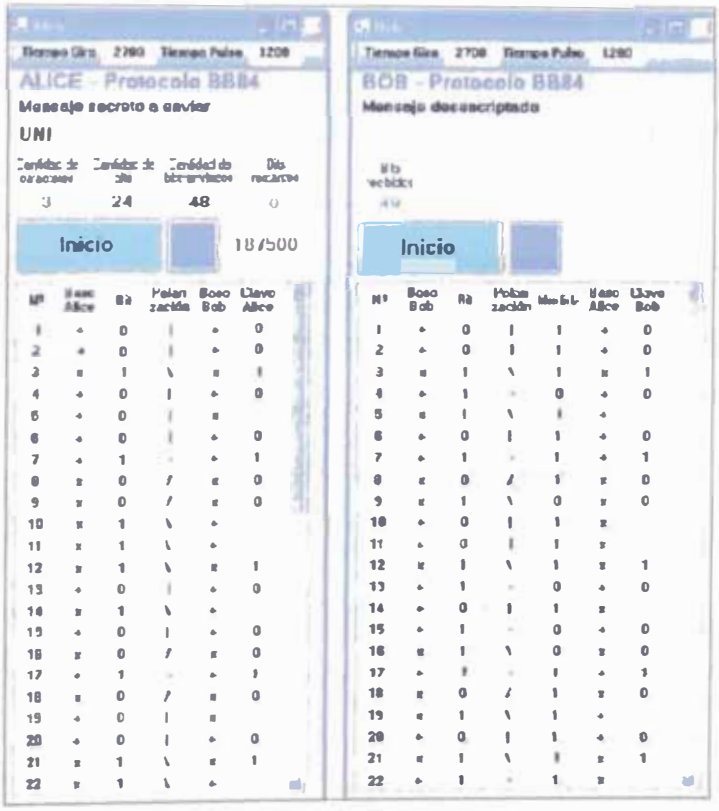


Figura 93: Alice y Bob construyen sus claves.

Alice simplemente selecciona los bits que corresponden a las polarizaciones que utilizó para enviar. En cambio Bob forma su clave siguiendo la siguiente regla, si su medida es "1" toma el bit que corresponde a la polarización que utilizó para medir, pero si es "0" toma el bit correspondiente a la polarización ortogonal a la que uso (Figura 93). Como se observa las claves obtenidas por Alice y Bob son iguales.

5. Luego Alice transforma el mensaje de texto a binario usando las equivalencias del código ASCII. Encripta el mensaje en binario usando su clave mediante el operador XOR y envía su resultado a Bob. Bob recibe el mensaje encriptado y le aplica su clave usando el operador XOR, obteniendo el mensaje en binario (Tal como lo realiza el programa de simulación). Finalmente lo convierte a texto usando las equivalencias de código ASCII (Figura 94).

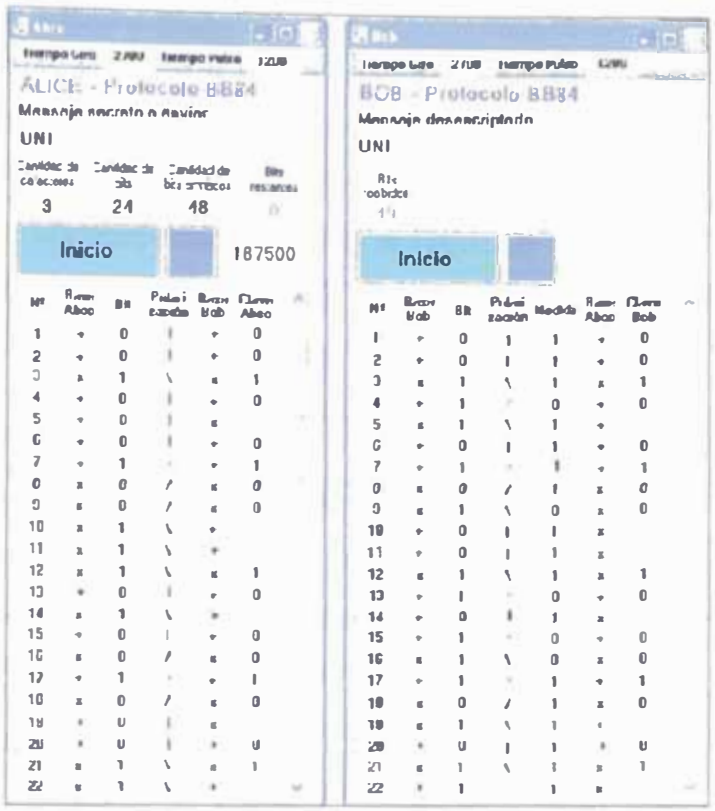


Figura 94: Alice envía el mensaje y Bob lo reconstruye.

En la Figura 95 se muestra el resto de bits, en total son transmitidos 48 bits, obteniéndose una clave sin procesar de 27 bits (56.25% del total). El software elimina los bits sobrantes y sólo toma en cuenta los primeros 24 bits necesarios para transmitir el mensaje secreto UNI.

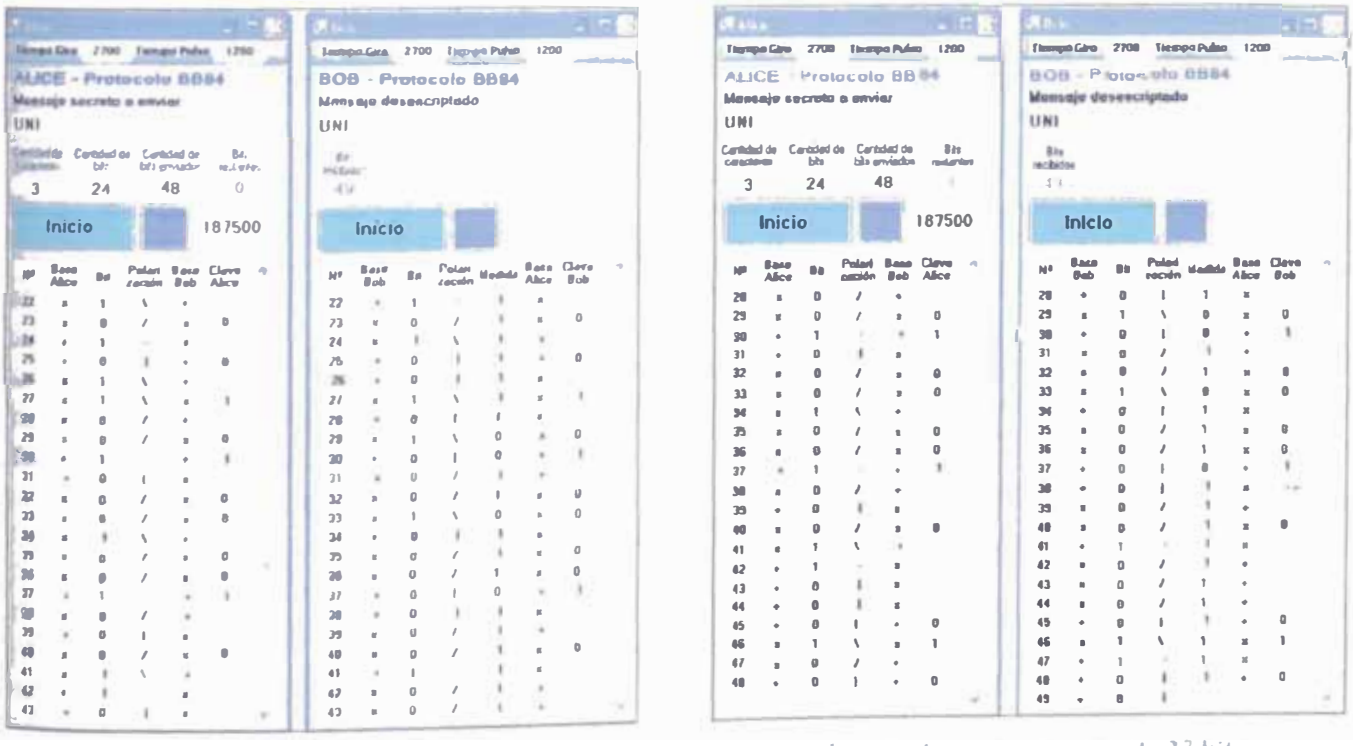


Figura 95: En total son 48 bits que Alice envía a Bob, formando una clave sin procesar de 27 bits.

Observaciones del programa de Alice y Bob:

- Los programas de Alice y Bob funcionan de manera independientes, esto quiere decir que no comparten variables ni funciones públicas de programación, lo único que los une es el canal clásico (el portapapeles) y el canal cuántico (el aire entre Alice y Bob). De esta forma si se tuviera una computadora exclusiva para Bob, solo se cambiaria el canal clásico y en vez del portapapeles se podria usar una red inalámbrica o cableada.

- El botón morado muestra en el formulario de Alice el mensaje en binario, la clave de Alice y el mensaje encriptado que envía al portapapeles. En la ventana de Bob aparece el mensaje encriptado recuperado del portapapeles, la clave de Bob y el mensaje desencriptado en binario (Figura 96). Si la clave es más grande que el mensaje se recorta y si es más pequeña se completa con los primeros bits. La clave final así formada siempre es la mitad de la cantidad de bits enviados.

Figura 96: Clave final la que se usará para encriptar. A) Los primeros 22 bits de la clave. B) Los 2 ultimos bits de la clave.

Programa de resumen del experimento:

Adicionalmente se cuenta con un programa que resume en un solo formulario los resultados del experimento. Se ejecuta el programa Resultados.exe y se hace clic en el botón "Mostrar Resultados" para ver el resumen del experimento (Figura 97).

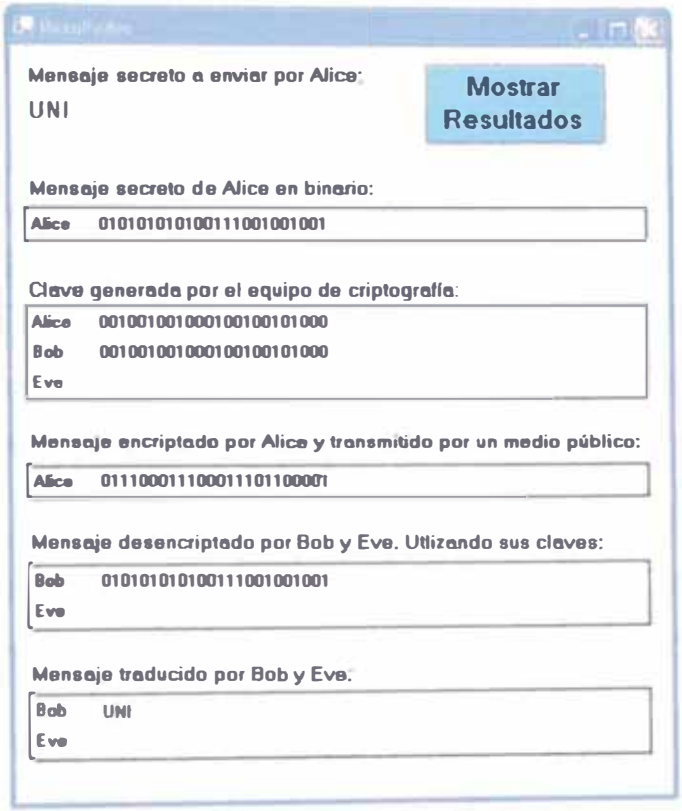


Figura 97: Resultado final de la distribución de claves usando el protocolo cuantico BB84. El mensaje se transmite sin dificultad.

7.2 Distribución de la clave con espía (Photon Number Splitting)

El método que se utilizó para espiar fue el de "dividir el número de fotones" (Photon Number Splitting), pero en vez de usar beamsplitters para dividir el haz, se utilizó dos vidrios comunes obteniendo resultados similares.

Como el equipo construido envía pulsos de fotones entonces Eve no tendrá inconveniente para descubrir la clave, pues el haz se dividirá en dos y tanto Eve como Bob recibirán fotones con la misma polarización Pero en el caso cuántico, cuando se trate de un fotón, el fotón no se podrá dividir y sólo ira por un camino, ya que el fotón en este experimento se comporta como partícula (Apéndice C). Por tanto la información que llegue a Bob sera alterada pues algunos fotones no llegarán

No obstante estos inconvenientes, los resultados obtenidos en este experimento demuestran que si es posible realizar una comunicación cuántica siempre y cuando el pulso se atenúe lo suficiente.

Descripción del aparato de interceptación:

Intruso o espía Eve: Está formado por dos polarizadores decodificadores fijos, uno con polarización vertical ↕ para medir en la base + y otro con polarización ⤢ para medir en la base × También tiene dos fototransistores y dos vidrios que simulan a los beamsplitters (Figura 98)

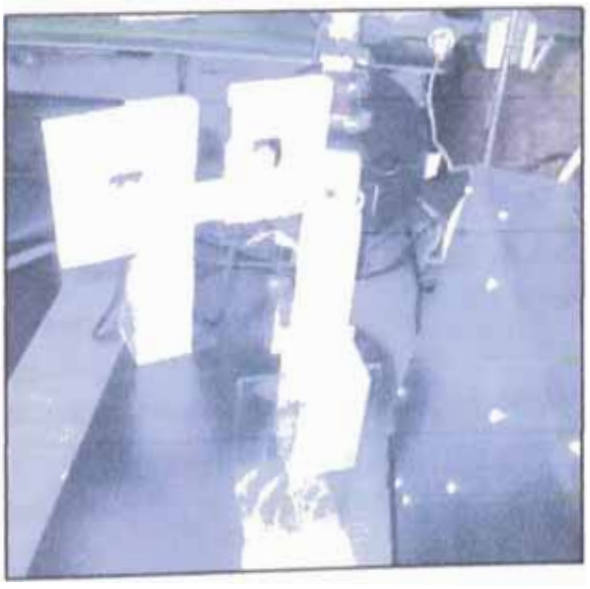


Figura 98: El espía Eve.

Descripción del experimento:

En la Figura 99 se muestra la "trayectoria" del laser. Se utilizó dos vidrios para desviar 2 veces el laser y obtener información de su polarización, pues se analiza en las 2 bases (rectilínea + y diagonal ×). En la Figura 100 se muestra la estrategia de ataque de Eve, ella utiliza 2 polarizadores para medir las con las polarizaciones ↕ y ↗ cada una correspondiente a las bases + y × respectivamente. A continuación se explica su funcionamiento:

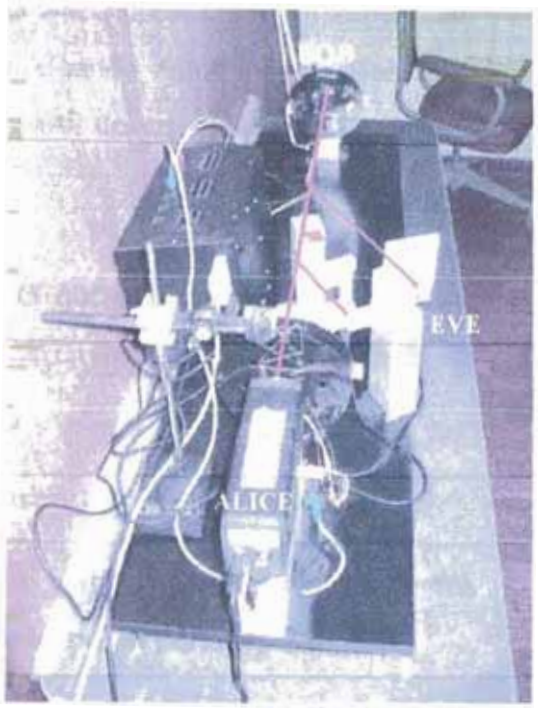


Figura 99: Las líneas rojas indican la "trayectoria" del laser para llegar a Bob y Eve.

Si Alice envía un pulso de fotones con polarización $|\updownarrow\rangle$, entonces siempre será detectada por la base × de Eve. Y también por su base +, pues ella mide con polarización ↕. De esta manera Eve acierta la polarización de envío de Alice. Pues Eve conoce la base de envío de Alice ya que se transmitió por un canal clásico

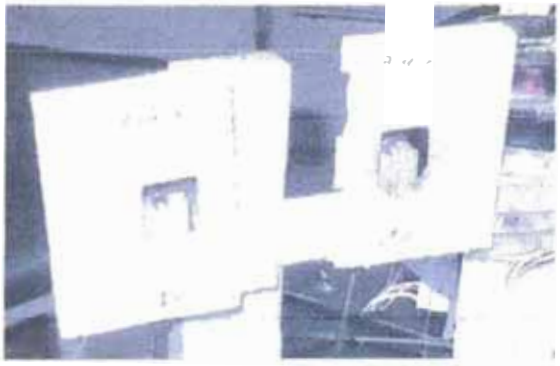


Figura 100: Polarizaciones que Eve utiliza para acertar la polarización que envía Alice.

Si Alice envía una polarización $|\leftrightarrow\rangle$, entonces siempre será detectada por la base × de Eve. Pero no será detectada por su base +, pues ella mide con polarización ↕. Entonces Eve razona de la siguiente manera "Si no se detecta entonces significa que se bloqueo, por tanto la polarización de Alice es ↔" y acierta.

Estos 2 resultados los obtiene por cada pulso pues el laser es dividido 2 veces. Situación que sería imposible si sólo se tratara de un fotón.

De esta forma Eve puede saber que polarización $|\updownarrow\rangle$ o $|\leftrightarrow\rangle$ empleo Alice.

De forma similar se puede describir el caso cuando Alice envía una polarización $|\nearrow\rangle$ o $|\nwarrow\rangle$.

¿Cómo sabe Eve cuando empezar a medir?

Al igual que Bob. Eve siempre está con sus instrumentos encendidos en espera del primer pulso que indique el inicio de la transmisión. Cuando Alice avise a Bob, Eve intercepta este pulso y sabrá que la transmisión será a partir del siguiente pulso.

¿Cómo sabe Eve cuando detenerse?

Eve siempre está observando lo que se publica en el portapapeles (canal clásico) y cuando detecta el mensaje de finalización que Alice envía a Bob, ella también se detendrá.

¿Cómo obtiene el mensaje encriptado?

Eve siempre observa lo que se transmita por el canal público (portapapeles), de esa manera obtiene el mensaje encriptado que Alice transmita por el portapapeles.

Resultados del experimento:

El equipo construido envía pulsos de fotones por lo que es factible que un espía obtenga la clave pues tiene suficientes fotones para analizar. Para la demostración se construirá una clave de 24 bits, suficiente para luego transmitir un mensaje de 3 caracteres.

1. Se ejecutan los programas Alice.exe, Bob.exe y Eve.exe. Se presiona el botón "Inicio" de Bob y Eve. En el primer formulario "Alice" se escribe el mensaje secreto que desea enviar, por ejemplo "UNI".
2. Alice y Bob trabajan exactamente igual al caso sin espía.
3. El tercer formulario corresponde a "Eve", ella utiliza dos polarizaciones ↕ y ↗ para medir la polarización reflejada por los vidrios mediante dos fototransistores que envían la medida al programa para ser procesada, si detecto anota "1" y si no detecto anota "0".
4. Alice y Bob construyen su clave exactamente como en el caso sin espía. Como Eve tiene acceso al canal clásico entonces construye su clave con las polarizaciones que corresponden al caso cuando las bases de Alice y Bob son iguales. Si Eve acertó la base y midió "1" entonces su bit será el que corresponde a la polarización usada. Si Eve acertó la base y midió "0" entonces su bit será el que corresponde a la polarización ortogonal (Figura 101 y 102).

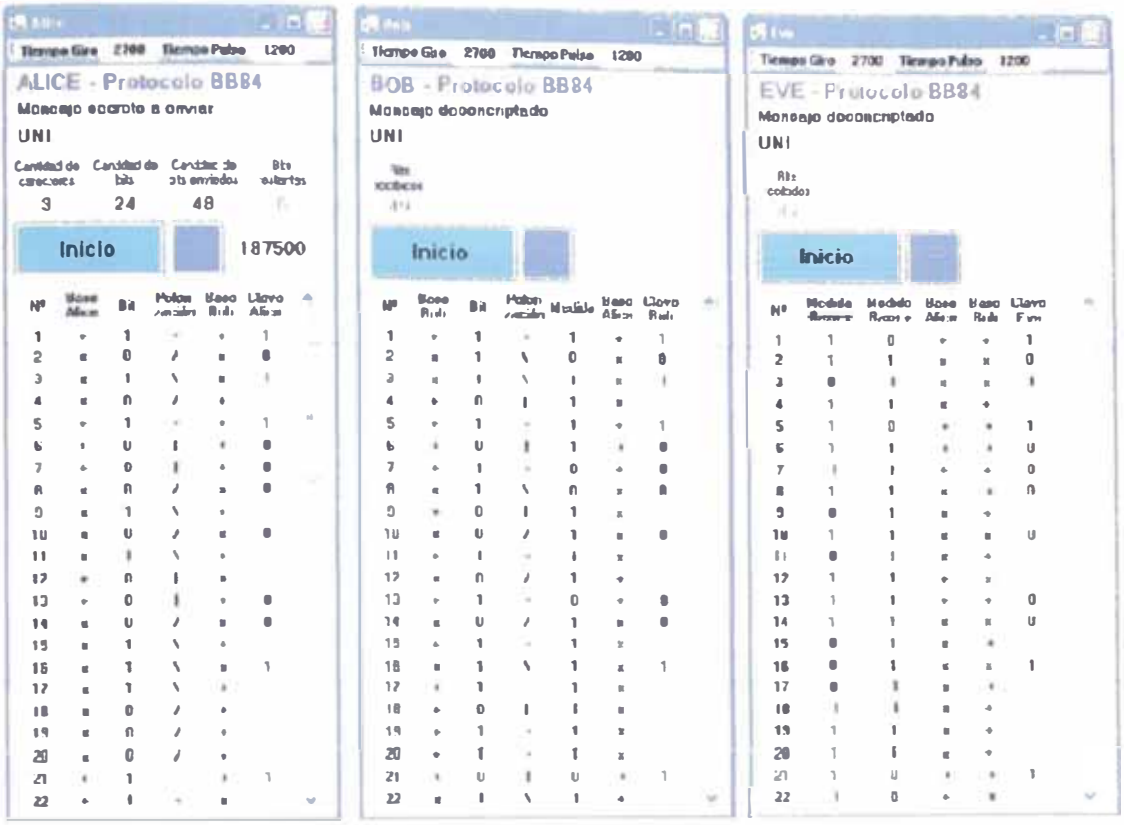


Figura 101: Los primeros 22 bits del experimento. La maquina envia pulsos de fotones por eso Eve logra obtener la misma informacion que llega a Bob.

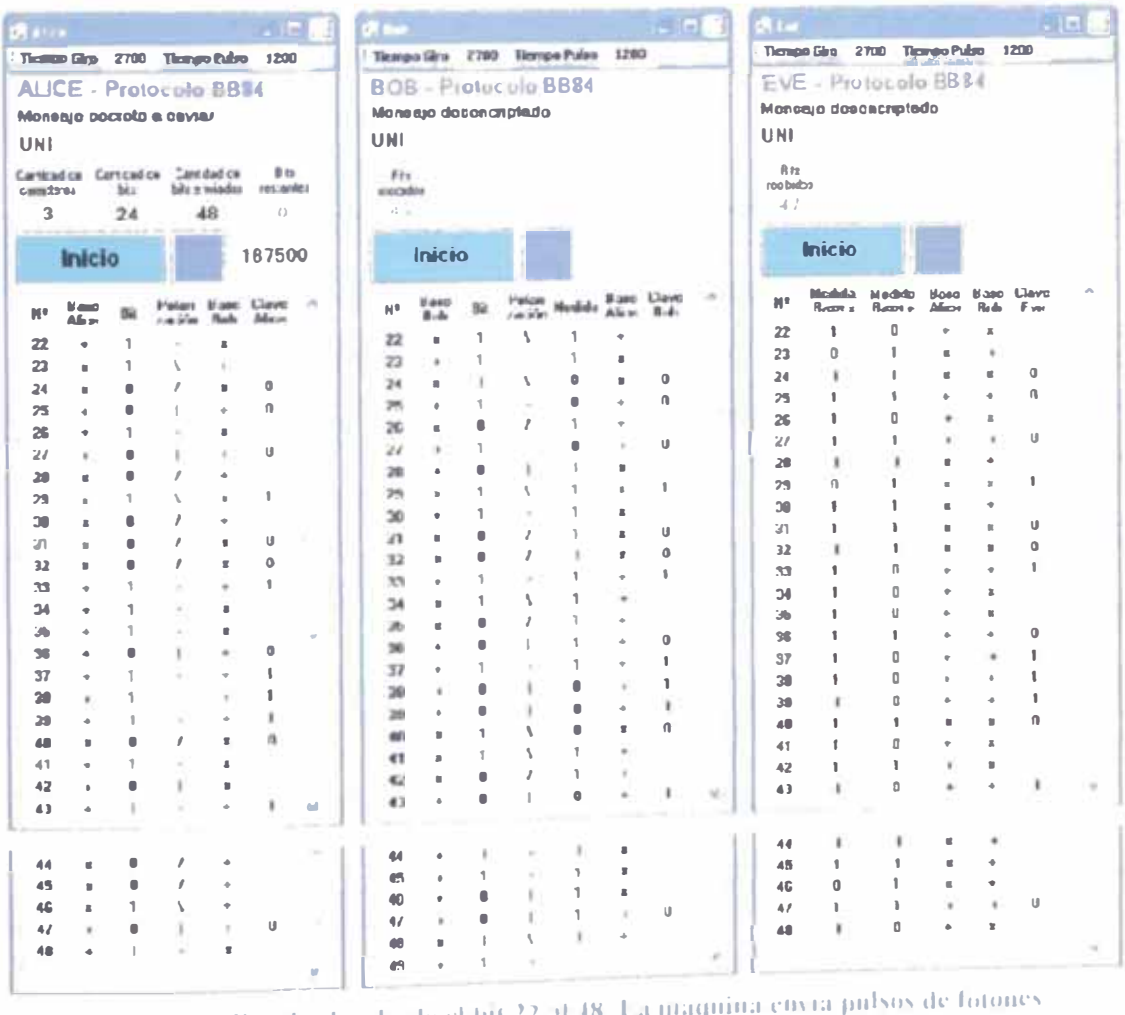


Figura 102: Resultados desde el bit 22 al 48. La maquina envia pulsos de fotones por eso Eve logra obtener la misma informacion que llega a Bob.

5. Como el haz es dividido en dos, Eve logra obtener la clave sin dificultad (Figura 103). Al igual que Alice y Bob si la clave de Eve es más grande se recorta y si es más pequeña se completa con los primeros bits. La clave final así formada siempre es la mitad de la cantidad de bits enviados.

Figura 103: Clave formada por Alice, Bob y Eve. Son las mismas.

6. En la Figura 104 se muestra el resumen del experimento.

Figura 104: Resultado final de la encriptación usando el protocolo BB84. El espía ob clave y descifra el mensaje.

7.3 Distribución de la clave con espía atenuando la intensidad del haz láser

Con la atenuación de la intensidad del pulso láser se disminuye controladamente la cantidad de fotones transmitidos. De tal forma que Bob y Eve tendrán dificultades en la detección, sin embargo en este experimento Eve será el más afectado pues el vidrio refleja menos del 50% (Apéndice C)

El equipo láser utilizado proporciona una potencia de 1 mW y está polarizado linealmente. Al colocar el polarizador del atenuador construido en paralelo, la potencia de salida se reduce[59] a 0.98 mW. El atenuador permite girar el polarizador un ángulo α entonces la potencia de salida final será de 0.98 cos α mW.

El atenuador construido tiene 18 divisiones de 20° cada una y experimentalmente se atenuó el láser para observar los efectos en la generación de la clave en Bob y en el espía Eve. El láser Helio-Neon tiene longitud de onda de $\lambda = 633$ nm y el tiempo del pulso de la máquina es de t = 1200 ms Como c = 3×10^8 m/s y h = 6 63 $\times$ 10^{-34} J.s se puede calcular el número de fotones por pulso y tabular (Tabla 9) el efecto en las claves de Bob y Eve.

Marca de rotación	Ángulo de rotación α (sexagesimales)	Potencia de Salida P = 0.98 cosα (mW)	Número de fotones por pulso $N = \frac{P}{hf}t = \frac{Pt\lambda}{hc}$	Efecto en la clave de Bob	Efecto en la clave de Eve
0	0°	0.98	3.74E+15	Clave correcta	Clave correcta
1	20°	0.92	3.52E+15	Clave correcta	Clave correcta
1.5	30°	0.85	3.24E+15	Clave correcta	Clave correcta
1.75	35°	0.80	3.07E+15	Clave correcta	Clave correcta
2	40°	0.75	2.87E+15	Clave correcta	Clave correcta
2.25	45°	0.69	2.65E+15	Clave correcta	Clave correcta. Con errores que no influyen en la clave[60]
2.5	50°	0.63	2.41E+15	Clave correcta	Clave correcta. Con errores que no influyen en la clave

[59] Según las características técnicas del polarizador adquirido (Instruction Polarizing Sheet for the PASCO Model OS-9477) la transmitancia en paralelo es aproximadamente 98%.

[60] El error ocurre en la base que no corresponden a la polarización de Alice, como Eva no toma en cuenta esta base, sino la base de su otro polarizador, entonces no influye en la clave deducida por Eve.

2.75	55°	0.56	2.15E+15	Clave correcta	Clave incorrecta. Algunos caracteres no son descifrados
3	60°	0.49	1.87E+15	Clave correcta	Clave incorrecta. La mayoría de veces no descifra ningún carácter
3.25	65°	0.41	1.58E+15	Clave correcta	Clave incorrecta. Problemas en la detección inicial, no se descifra ningún carácter. Algunas veces no detecta la señal
3.5	70°	0.34	1.28E+15	Clave incorrecta. Algunos caracteres no son descifrados	No detecta señal
3.75	75°	0.25	9.69E+14	No detecta señal	No detecta señal

Tabla 9: Efectos en las claves al reducir la potencia del pulso láser.

En la tabla anterior se puede observar claramente que a partir de 55° la interceptación del espía es ineficaz, permitiendo todavia que Bob obtenga la clave correcta. Esto muestra la necesidad de utilizar en estos sistemas fuentes láser de muy baja potencia con, obviamente, detectores de alta sensibilidad Esto en el límite conduce a la utilización de fuentes y detectores de fotones individuales (Apéndice C) que se están implementando en la tecnología del mundo desarrollado.

La máquina construida no está sobre un banco óptico. Los soportes que sostienen los vidrios están colocados manualmente sobre marcas en el tablero por lo que cada vez que se repita el experimento los resultados mostrados en la Tabla 9 pueden cambiar ligeramente.

A continuación se muestra el caso cuando $\alpha = 55°$ (P=0 56 mW). El espía solo descubre parte de la clave y obtiene sólo una letra del mensaje (Figura 105).

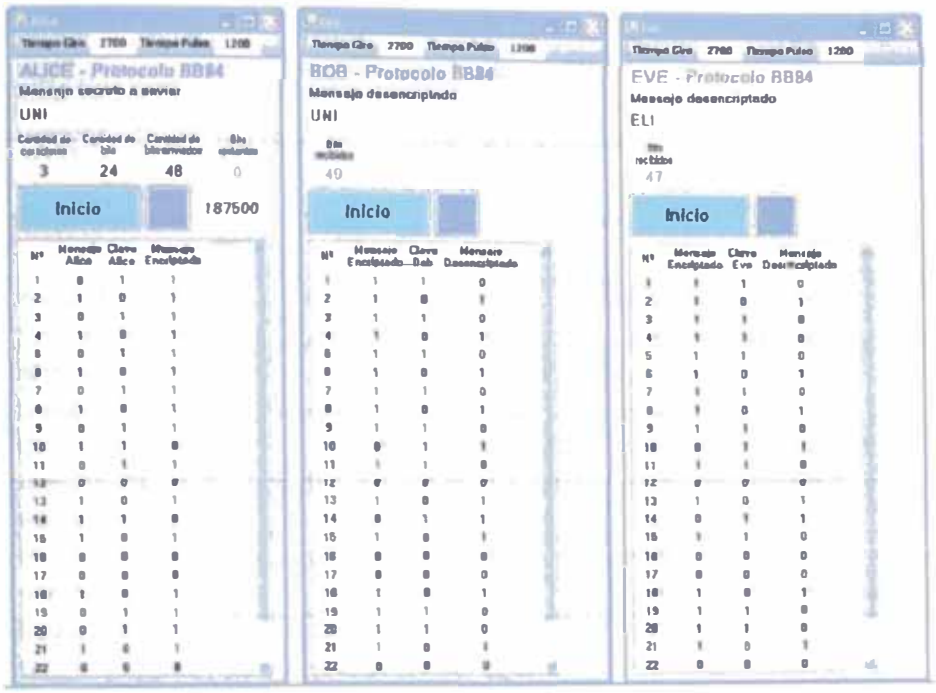


Figura 105: Al atenuar el laser, los fototransistores de Eve tienen dificultad para registrar el pulso laser.

A medida que se atenúa más la potencia del laser, Eve tendrá mayor dificultad para obtener la clave. En la Figura 106 se muestra como a una mayor atenuación, $\alpha = 60°$ (P=0.49 mW) Eve obtiene un mensaje ilegible.

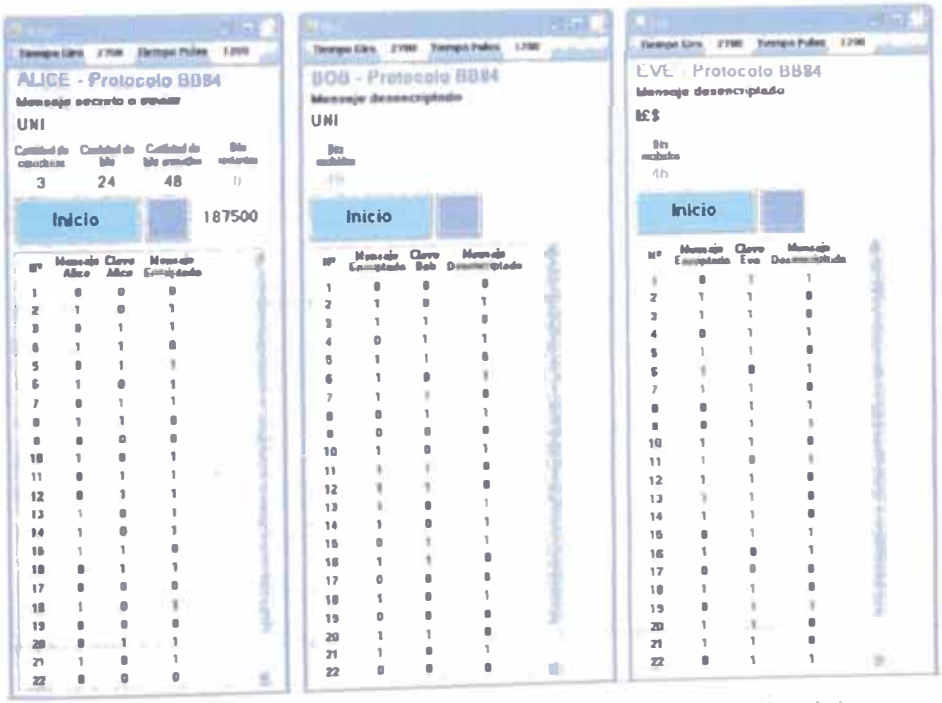


Figura 106: Si el laser se atenúa más, los fototransistores de Eve dejaran de detectar muchas señales y generaran una clave distinta.

Incluso se puede llegar al límite en que Eve no detecte ninguna señal, $\alpha = 65°$ (P=0.41 mW) (Figura 107).

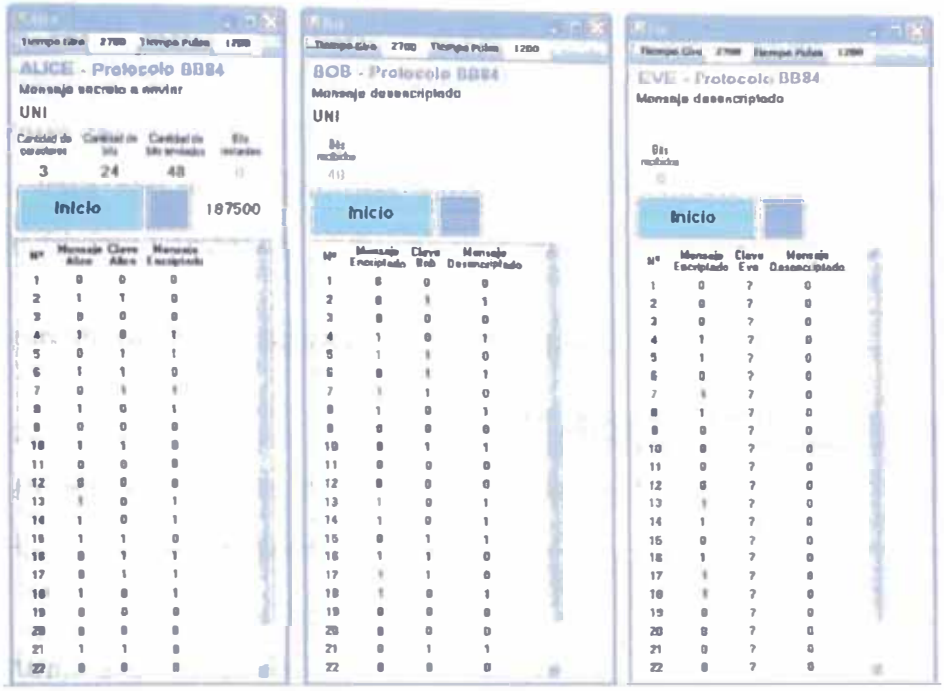


Figura 107: Eve no detecto señal.

7.4 Uso de la máquina para enviar un mensaje

Una vez construida la clave, también se puede usar la máquina para enviar el mensaje encriptado. Para ello se escribió dos programas, uno para el emisor y otro para el receptor. Partes importantes del código se muestran en el Apéndice D.

Funcionamiento del programa Emisor Alice

1. Una vez obtenida la clave, Alice está listo para enviar cualquier mensaje de igual longitud de la clave En la Figura 108 se muestra el caso de una clave para cuatro caracteres.

2 En el cuadro "Clave" se copia la clave que se obtuvo mediante el protocolo BB84.

3. En el cuadro "Mensaje secreto a enviar" se escribe un mensaje con un número de caracteres que corresponda a la clave (un carácter es representado por 8 bits).

Figura 108: Emisor Alice.

4. El programa convierte el mensaje secreto a binario y aplica la operación XOR al mensaje en binario y a la clave para obtener el mensaje codificado.

5. El disco de Alice está alineado para una polarización vertical ↕ y el chopper está bloqueando el láser Para iniciar la transmisión se hace clic al botón "Iniciar Envío".

6. El chopper gira y deja pasar un pulso, ese pulso llega a Bob indicándole que se iniciará la transmisión del mensaje codificado en 25 ms. Bob tomará sus datos a partir del segundo pulso.

7. Si el bit codificado es "1" el programa gira el chopper y envía la polarización vertical ↕ y si el bit codificado es "0" no gira el chopper y no envía pulso. Este

proceso tiene un periodo de 175 ms (150 ms para el siguiente análisis y 25 ms de giro o reposo según sea el bit codificado).

Funcionamiento del programa Receptor Bob

1. Una vez obtenida la clave, Bob está listo para recepcionar cualquier mensaje de igual longitud de la clave. En la Figura 109 se muestra el caso de una clave para cuatro caracteres.

Figura 109: Receptor Bob.

2. En el cuadro "Clave" se copia la clave que se obtuvo mediante el protocolo BB84.

3. El disco de Bob está alineado para una polarización vertical ↕.

4. Para activar el fototransistor y esperar la señal de inicio de transmisión de Alice, Bob hace clic al botón "Iniciar Recepción".

5. Cuando el programa detecta un pulso láser significa que Alice iniciará el envío del mensaje codificado en 25 ms. Bob tomará como dato a partir de la siguiente señal pues la primera solo sirvió para avisarle que iniciará la transmisión.

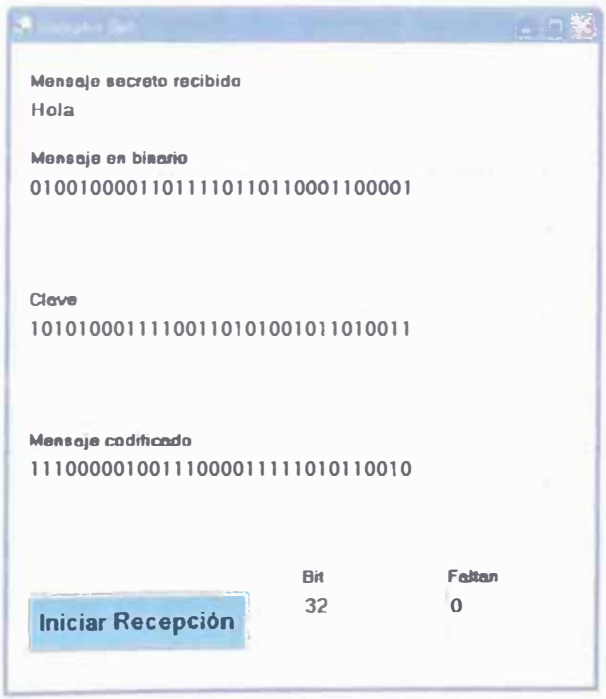


Figura 110: Bob recibe el mensaje con exito.

6. Si Bob detecta una señal significa que Alice envió el bit "1" y si no detecta, significa que tiene el bit "0" Este proceso tiene un periodo de 175 ms (150 ms con el detector apagado y luego 25 ms con el detector encendido).

7.5 Resumen de resultados experimentales

1. Se ha construido un equipo básico experimental, cuya electromecánica es controlada por computadora, que permite aplicar el protocolo cuántico BB84 para distribuir por aire libre una clave secreta a una distancia de 1.5 m. Los resultados obtenidos coinciden con los esperados teóricamente, es decir que la clave obtenida está formada por aproximadamente el 50% de los bits usados por Alice (Página 152).

2. Debido a que la máquina utiliza pulsos intensos de fotones (**no fotones individuales**) se observa que el método de ataque de dividir el número de fotones (Photon Number Splitting) tiene éxito Sin embargo cuando se atenúa fuertemente la intensidad del pulso laser se llega a un limite, a partir del cual Bob puede todavía obtener la clave correcta en tanto que Eve tiene cada vez más dificultades en detectar señal Es en esta ruta que se encuentra la seguridad cuántica en la que se está trabajando en laboratorios extranjeros más avanzados. Estos están construyendo actualmente fuentes láser de fotones individuales (single photon sources) y detectores de fotones individuales (single photon detectors) que permitan utilizar directamente el principio de la Mecánica Cuántica que señala que cualquier intervención en el fotón (por medición de sus propiedades fisicas) modifica sus estado inicial.

3. Este proyecto básico es el primer paso en la construcción de un equipo más sofisticado. Los resultados y la experiencia obtenida nos permite proyectar un nuevo prototipo para realizar comunicación cuántica a gran escala, es decir distribución de claves de mayor tamaño (del orden de kilobits) a mayores distancias (del orden de kilómetros).

4. Este trabajo de simulación y experimentación multidisciplinaria nos muestra que es posible en nuestro medio, aún con poco presupuesto, iniciar investigaciones avanzadas en temas novedosos y con tecnología de punta que aplican principios de las Ciencias Básicas

Capítulo 8

Diseño de un Proyecto Futuro

En esta sección se presenta un proyecto accesible a un presupuesto en nuestro medio. Se tiene los conocimientos físicos y técnicos necesarios para construir una máquina de criptografía cuántica real.

El prototipo que se ha construido presenta tres grandes problemas: el laser envía un pulso de fotones, la electromecánica es lenta y el sistema detección no es eficiente.

En las Figura 111, 112 y 113 se presenta un prototipo construido por Henning Weier (32), logrando transmitir a 0.5 Km. en un medio urbano usando el protocolo BB84.

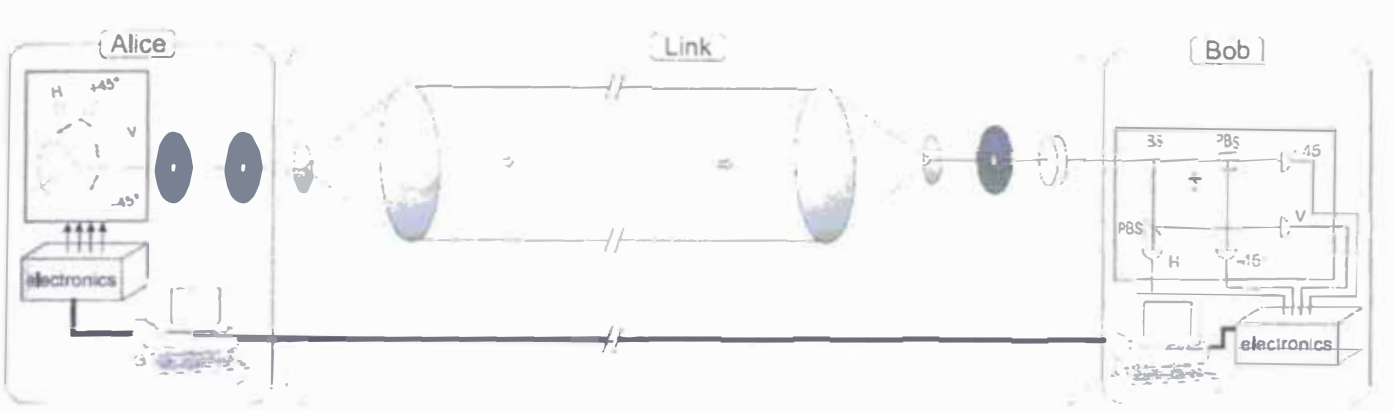


Figura 111: Esquema del sistema de criptografía cuántica. Se divide en tres partes: Emisor (Alice), Enlace de transmisión (Link) y el Receptor (Bob).

El Emisor (Alice): El diseño para Alice tiene cuatro diodos láser polarizados de 850 nm los cuales son controlados por un reloj de *10 Mhz* para disparar pulsos de fotones a un espejo cónico. Estos pulsos son atenuados hasta alcanzar una media en el número de fotones de $\mu - 0.1$ (Apéndice C) por medida, para ello utiliza potenciómetros para ajustar el voltaje de los diodos láser y laminas atenuadoras.

Además Alice tiene un quinto láser más potente que utiliza para efectos de alineamiento con los detectores de Bob

Después de que el pulso ha sido reflejado por el espejo cónico, pasa por un filtro espacial que asegura su alineación. Este filtro está formado por dos pequeños agujeros (pinholes) de 100 μm separados 9 mm. Para lograr que el pulso se concentre en los

pinholes se coloca un lente convergente de distancia focal 2.75 mm entre el espejo cónico y los pinhole.

Canal cuántico (Link): Cuando el pulso sale del filtro espacial de Alice, este llega al sistema de lentes mostrado en la Figura 112. Esto es necesario para asegurar que la mayor cantidad de fotones enviados por Alice sean detectados por Bob.

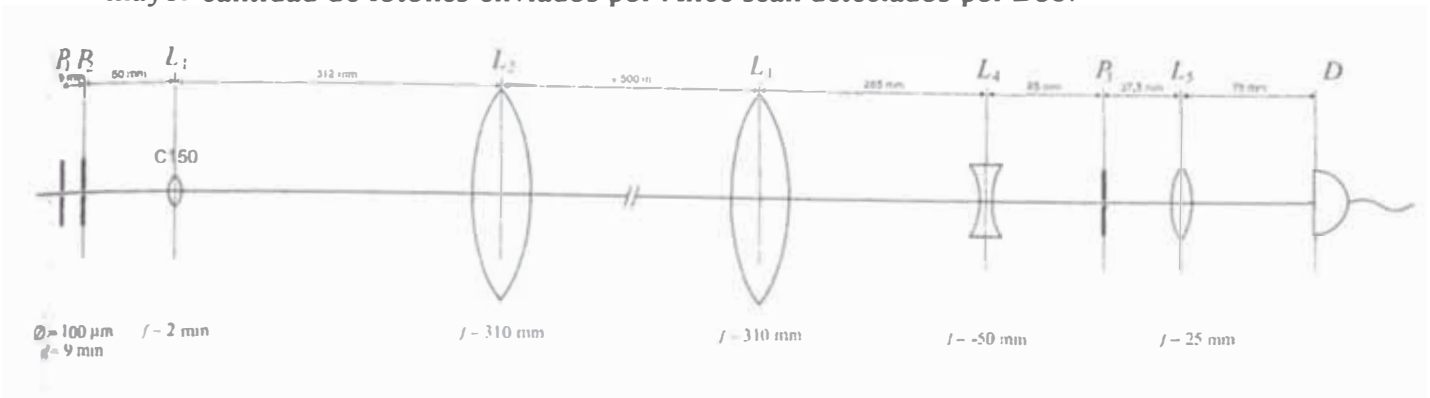


Figura 112: Sistema de lentes del enlace de transmisión.

Con el fin de concentrar el pulso que sale del filtro espacial se coloca a 50 mm un lente convexo (convergente) L_1 de distancia focal de 2 mm, luego a 312 mm se coloca un lente L_2 de f = 310 mm, en el punto de destino a 500 m se coloca un lente igual L_3 de f = 310mm, luego a 285 mm un lente cóncavo (divergente) L_4 de f = -50 mm con el objetivo de lograr una abertura que encaje en el pinhole de 100 µm que se encuentra a 65 mm. Finalmente a 37.5 mm pasa por un lente L_5 de de f = 25 mm para concentrar nuevamente el pulso y dirigirlo al filtro espectral de Bob que se encuentra a 75 mm.

El Emisor (Bob): Antes de medir la polarización del fotón, este debe pasar por un filtro espectral que asegure que solo longitudes de onda de 850 nm lleguen al analizador. El analizador que permite medir aleatoriamente la polarización del fotón está formado por un beamsplitter no polarizador (BS), dos beamsplitter polarizadores (PBS), una lámina retardadora media onda ($\lambda/2$) rotado 22.5° y cuatro fotodiodos de avalancha de silicio (SiAPD) (Figura 113).

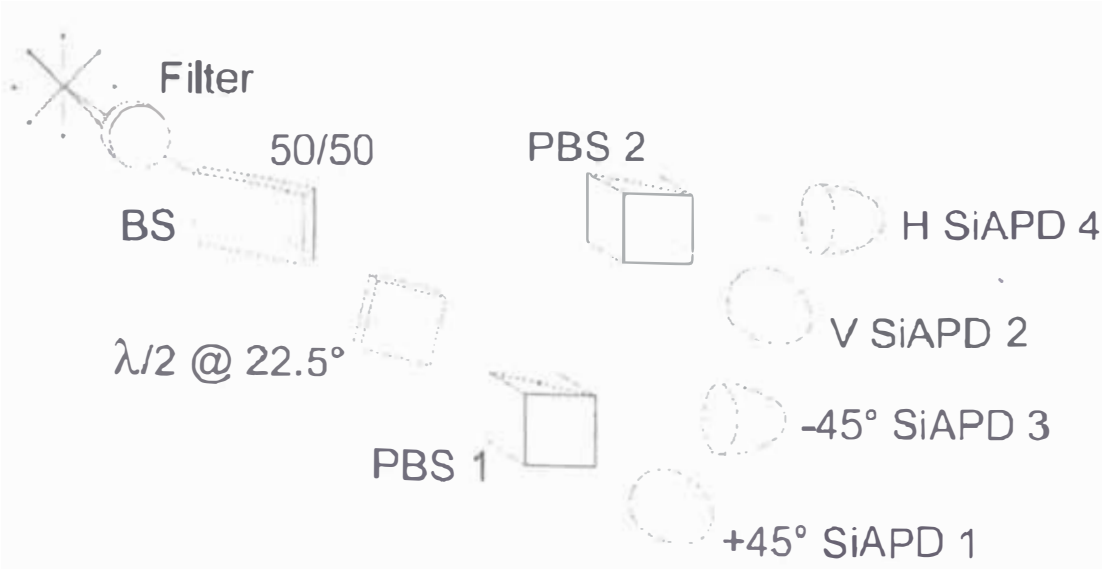


Figura 113: Componentes del analizador de Bob. Mide aleatoriamente la polarizacion del fotón

A continuación se explica su funcionamiento:

- Caso 1: El fotón llega al beamsplitter no polarizador BS y tiene una probabilidad del 50 % de llegar al beamsplitter polarizador PBS2[61], y si está en la base × tiene un 50 % de probabilidad de llegar al detector 2 ó 4 y si está en la base + un 100% de llegar sólo a un detector 2 ó 4.

- Caso 2: El fotón llega al beamsplitter BS y tiene una probabilidad del 50 % de llegar al filtro media onda (que rota 45° la polarización del fotón) y luego al PBS1, y si está en la base + tiene un 50 % de probabilidad de llegar al detector 1 ó 3 y si está en la base × un 100% de llegar sólo a un detector 1 ó 3.

- Estos dos casos aseguran la aleatoriedad de medida de Bob. Este esquema está basado en el diseño patentado de Rarity y Tapser (39). La explicación más detallada se encuentra en el Apéndice C.

Para un diseño futuro se tomaría como base este modelo, pero adaptándolo para implementar el protocolo B92 que requiere de menos componentes. El costo aproximado de construcción es de $ 50,000. La máquina construida para esta tesis costo aproximadamente $ 1,500.

[61] Como se muestra en el Apéndice C. Cuando el fotón pasa el primer beamsplitter realmente viaja simultáneamente por los dos caminos mientras no se le mida. Pero al medirlo colapsará como particula. Es por eso que en este análisis se trata al fotón desde el principio como particula.

Con un poco más de presupuesto se podrá construir una máquina que utilice el protocolo E91. Para ello se tendría principalmente que ensamblar una fuente de fotones entrelazados (40) utilizando la Conversión Paramétrica Espontanea Descendente (Apéndice C).

En la Figura 114 se muestra el diseño realizado por Kristin M. Beck y Jacob E. Mainzer en el 2008, donde utilizan cristales de β-Barium Borate (β-BaB_2O_4 o BBO) para producir dos fotones entrelazados. Este es un diseño prácticamente estándar.

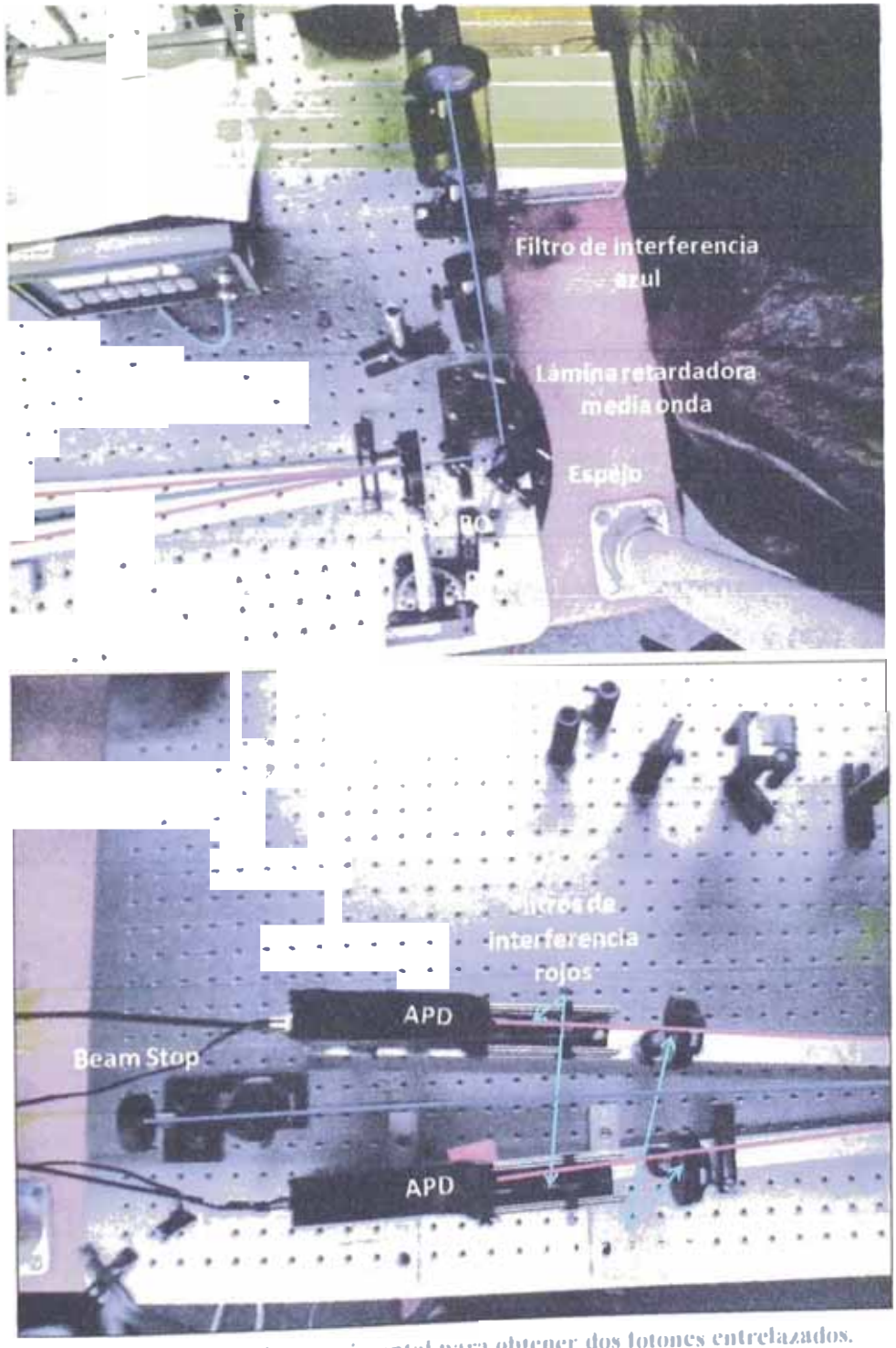


Figura 114: Montaje experimental para obtener dos fotones entrelazados.

El laser polarizado verticalmente $|\updownarrow\rangle$ llega a un filtro de interferencia azul que asegura la coherencia temporal. Luego llega a una lámina retardadora media onda que rota la polarización a 45°, $|\updownarrow\rangle = \frac{|\leftrightarrow\rangle + |\updownarrow\rangle}{\sqrt{2}}$, despues llega al espejo el cual lo dirige a dos cristales BBO para producir fotones entrelazados del tipo mostrado en la Figura 115 (Apéndice C).

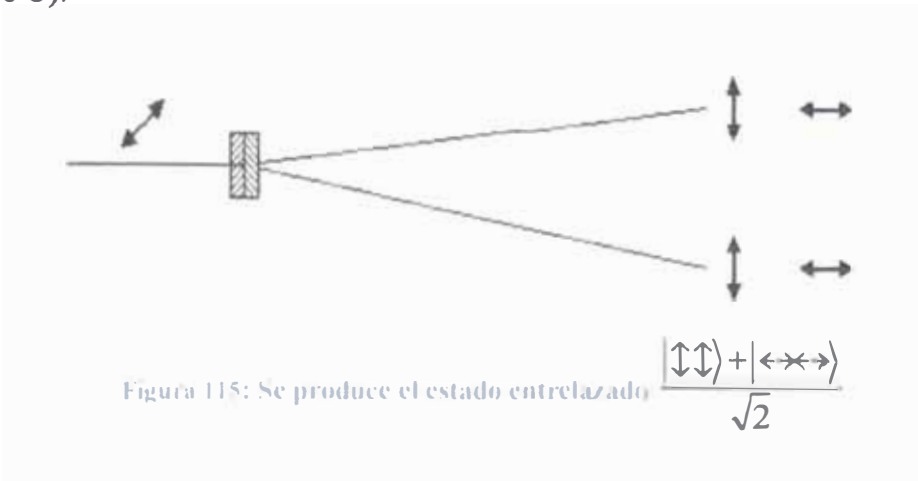


Figura 115: Se produce el estado entrelazado $\frac{|\updownarrow\updownarrow\rangle + |\leftrightarrow\leftrightarrow\rangle}{\sqrt{2}}$

El par de fotones generados pasan por unos polarizadores que colapsan el estado, para luego pasar por filtros de interferencia rojos para asegurarse que se tratan de los fotones generados por la Conversión Paramétrica Espontanea Descendente. Finalmente son medidos por los APD (Avalanche Photo Diode) (41) donde se comprueba experimentalmente la creación de pares de fotones entrelazados.

Además se podría usar el mismo aparato para iniciar experimentos prácticos en computación cuántica de fotones y teleportación de fotones (41) y (42). La primera teleportación cuántica de fotones se realizó en 1997 (43).

Capítulo 9

Conclusiones finales

Recientemente se ha introducido en la Facultad de Ciencias de la UNI el tema novedoso y contra-intuitivo de la Computación Cuántica a través de la enseñanza de los aspectos teóricos fundamentales y de esquemas de simulación computarizada.

El presente trabajo presenta una primera experiencia en nuestro medio de la aplicación de los conceptos cuánticos en el procesamiento codificado de la información, denominado Criptografía Cuántica.

1. En la primera parte de esta tesis se ha presentado los conceptos básicos de la Criptografía Clásica actual y se ha mostrado su potencial vulnerabilidad frente a la eficiencia de algoritmos cuánticos capaces de resolver problemas complejos como la factorización de números muy grandes, en los que se basa la seguridad en criptografía clásica (por ejemplo, algoritmo clásico RSA). También por primera vez en nuestro medio se ha introducido claramente las características teóricas y técnicas de los esquemas de criptografía cuántica que se encuentran en pleno desarrollo en el mundo. En el marco del protocolo cuántico BB84 se ha efectuado un detallado cálculo de las fórmulas probabilísticas que describen el intercambio de qubits entre el emisor Alice y el receptor Bob durante el proceso de Distribución de Clave Cuántica (QKD). Todo esto asumiendo una implementación física ideal y en presencia tanto de ruido instrumental o de transmisión como de interceptación o intervención del espía Eve.

2. El trabajo experimental propio de esta tesis está relacionada con la construcción de un equipo práctico que aplique el protocolo cuántico BB84, pero en medio de grandes limitaciones económicas, que obligaron a simplificar el prototipo y utilizar diseños propios con materiales de bajo costo. Este trabajo consiste de tres partes relacionadas:
   a. Se han deducido las fórmulas probabilísticas que gobiernan la transmisión de qubits en la máquina construida (párrafo 2.3.1.2). Estas fórmulas resultan ser iguales a los que se dedujo anteriormente para máquinas ideales, lo que demuestra que ambas máquinas en principio son equivalentes. Estas fórmulas

toman en cuenta tanto el ruido en la transmisión como el ataque de espias, por tanto son ecuaciones completas que describen cualquier caso de transmisión que utilice el protocolo cuántico BB84. Estas fórmulas ni las propias deducciones se encuentran publicadas en ningún artículo conocido, lo que es un aporte propio de esta tesis.

b. Se ha efectuado simulaciones en computadora clásica de los diversos aspectos del protocolo cuántico BB84, adaptados al diseño de la máquina construida y con la finalidad de comparar con los resultados calculados por las fórmulas teóricas. La ejecución de los programas (cuyos códigos se presentan en el Apéndice D) comprueban los cálculos teóricos dentro de las probabilidades esperadas. Por ejemplo, sin ataque o intervención del espía, el software muestra que la coincidencia de bases es aproximadamente el 50% de la cantidad de bases utilizadas por Alice, como se espera teóricamente. También muestra que los métodos de ataque siempre influyen en la formación de la clave de Bob, haciendo posible que Alice y Bob se percaten que han sido espiados. Esto da una idea de la seguridad del protocolo y muestra que Eve tiene una bajísima probabilidad de acertar en la definición de un carácter alfanumérico, obteniendo siempre mensajes ilegibles (0 29% en el método de interceptación "Man in the Middle" (MITM) y un porcentaje similar en el método "Photon Number Splitting" (PNS), en este ultimo caso dependiendo del porcentaje de desvío).

c. Se ha construido un equipo básico experimental, cuya electromecánica es también controlada por la computadora, que permite aplicar el protocolo cuántico BB84 para distribuir por aire libre una clave secreta a una distancia de 1.5 m. Los resultados obtenidos coinciden con los esperados teóricamente, es decir que la clave obtenida está formada por aproximadamente el 50% de los bits usados por Alice.

d. Debido a que la máquina utiliza pulsos intensos de fotones (**no fotones individuales**) se observa que el método de ataque implementado de dividir el número de fotones (Photon Number Splitting) tiene éxito. Sin embargo cuando se atenúa fuertemente la intensidad del pulso laser se llega a un límite, a partir del cual Bob puede todavía obtener la clave correcta en tanto que Eve tiene cada vez más dificultades en detectar señal. Es en esta ruta que se encuentra la

seguridad cuántica en la que se está trabajando en laboratorios extranjeros más avanzados. Estos están construyendo actualmente fuentes láser de fotones individuales (single photon sources) y detectores de fotones individuales (single photon detectors) que permitan utilizar directamente el principio de la Mecánica Cuántica que señala que cualquier intervención en el fotón (por medición de sus propiedades físicas) modifica su estado inicial.

3. Este proyecto es el primer paso en la construcción de un equipo más sofisticado. Los resultados y la experiencia obtenida nos permite proyectar un nuevo prototipo para realizar comunicación cuántica a gran escala, es decir distribución de claves de mayor tamaño (del orden de kilobits) a mayores distancias (del orden de kilómetros). Un posible diseño se muestra en el Capítulo 8. Este es el camino que están siguiendo muchas las instituciones científicas dedicadas a este tema, con diferentes presupuestos

4. Este trabajo de simulación y experimentación multidisciplinaria nos muestra que es posible en nuestro medio, aún con poco presupuesto, iniciar investigaciones avanzadas en temas novedosos y con tecnología de punta, aplicando principios de las Ciencias Básicas.

Bibliografía

1. **www.qubit.org.** : Centro de Computación Cuántica de la Universidad de Oxford.

2. **Ignacio Cirac, Director del Instituto Max Planck de Óptica Cuántica de Munich.** : Noticias EFE, 25 de febrero del 2009.

3. **Shor, Peter W.** *Algorithms for Quantum Computation: Discrete Logarithms and Factoring.* : 35th Annual Symposium on Foundations of Computer Science, 1994.

4. **W. Merkel, I. Averbukh, B. Girard, G. Paulus.** *Factorization of numbers with physical systems.* : Fortschritte der Physik 54, Nos 8-10, p. 856-865, 2006.

5. **Feynman, Richard P.** *Simulating Physics with Computers.* : International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982.

6. **Grover, L.** *A fast quantum mechanical algorithm for database search.* : 28th Annual ACM Symposium on Theory of Computing, 1996.

7. **Aram W. Harrow, Avinatan Hassidim and Seth Lloyd.** *Quantum algorithm for solving linear systems of equations.* . Universidad de Bristol y MIT, 19 de noviembre del 2008.

8. **R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson.** *Practical free-space quantum key distribution over 10 km in daylight and at night.* : New Journal of Physics 4, pag. 43, 2002.

9. **C. H. Bennett, G. Brassard.** *Quantum Cryptography Public Key Distribution and Coin Tossing.* : International Conference on Computers, Systems and Signal Processing, diciembre de 1984

10. **C. H. Bennet, G. Brassard.** *The dawn of a new era for quantum cryptography: The experimental prototype is working.* : Sigact News, Vol. 20, N° 4, pág. 78 - 82, 1989.

11. **Tobias Schmitt-Manderbach, HenningWeier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter.** *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km.* Physical Review Letters 98, 05 de enero del 2007.

12. **R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheid, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger.** *Entanglement-based quantum communication over 144km.* : Nature Physics, 3 de junio del 2007.

13. **Javier Aretio Bertolín, Director del Grupo de Investigación en Redes y Sistemas de la Universidad de Deusto.** *La criptografía cuántica una tecnología clave para la seguridad en red.* : Revista Seguridad en Redes, Octubre 2008.

14. **Donna Dodson (NIST), Mikio Fujiwara (NICT), Philippe Grangier (CNRS), Masahito Hayashi (Tohoku University), Kentaro Imafuku (AIST), Ken-ichi Kitayama (Osaka University), Prem Kumar (Northwestern University), Christian Kurtsiefer (National University of Si.** *Updating Quantum Cryptography Report ver. 1.* : s n., Mayo 2009.

15. **Koenig, Kelly.** *Nanotechnological Applications in Quantum Cryptography.* : s.n., Abril 2009.

16. **Shannon, Claude.** *Communication Theory of Secrecy Systems.* : Bell System Technical Journal 28, 4· 656-715, 1949

17. **Samuel J. Lomonoco, Jr.** *A Quick Glance at Quantum Cryptography.* Universidad de Maryland, Baltimore County, 8 de noviembre de 1998.

18. **Laboratories, RSA.** *Frequently Asked Questions about Today's Cryptography.* RSA Security Inc., http://www.rsasecurity.com, Mayo 2000.

19. **Laboratories, RSA.** *The RSA-640 is factored.* : RSA Security Inc. http:www.rsasecurity.com/rsalabs/node.asp?id=2092, 2 de noviembre del 2005.

20. **Paine, Steve Burnett and Stephen.** *RSA Security's Official Guide to Cryptography.* : Osborne/McGraw-Hill, 2001

21. **Hughes, Richard J.** *Cryptography, Quantum Computation and Trapped Ions.* : Los Alamos National Laboratory, 1997.

22. **Gerjuoy, Edward.** *Shor's Factoring Algorithm and Modern Cryptography. An Illustration of the Capabilities Inherent in Quantum Computers.* : Dept. of Physics, University of Pittsburgh, noviembre 2004.

23. **Hayward, Matthew.** *Quantum Computing and Shor's Algorithm.* : s.n., 2005.

24. **Hams, Anthony.** *Quantum Computation and Spin Manipulation.* : Universidad Groningen, Holanda, Tesis de Doctor en Física, 2002.

25. **W. K. Wootters, W. H. Zurek.** *A single quantum cannot be cloned.* : Nature, Vol. 299, No. 5886, pág 802-803, 28 de octubre de 1982.

26. **Hardies, P. W. Milonni and M. L.** *Photons cannot always be replicated.* Physics. Lett. A 92, 321-322, 1982.

27. **Shor, Peter W. y Preskill, John.** *Simple proof of security of the BB84 quantum key distribution protocol.* : Physical Review Letters, 85, 441–444, 2000.

28. **Papanikolaou, Nikolaos K.** *Techniques for Design and Validation of Quantum Protocols.* . Universidad de Warwick, Inglaterra. Tesis de Maestría en Ciencias, 2004.

29. **Ma, Xiongfeng.** *Quantum Cryptography: From Theory to Practice.* : Universidad de Toronto, Canada. Tesis de Doctor en Física, 2008.

30. **Erven, Chris.** *On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source.* : Universidad de Waterloo. Tesis de Maestría en Ciencias Físicas. http://www.iqc ca/publications/theses/cerven.pdf, 2007.

31. **Schmitt-Manderbach, Tobias.** *Long distance free-space quantum key distribution.* : Universidad Ludwig–Maximilians de Munich. Tesis de Doctor en Física. http://xqp.physik.uni-muenchen.de/publ/Schmitt_Manderbach.pdf, 2007.

32. **Weier, Henning.** *Experimental Quantum Cryptography.* : Universidad Técnica de Munich. Tesis de Diplomado en Física. http://xqp.physik.uni-muenchen.de/publ/henning-diplom.pdf, 2003.

33. **Hendrych, Martin.** *Experimental Quantum Cryptography.* : Universidad de Olomouc, República Checa. Tesis para optar el grado de Doctor en Física. http://optics.upol.cz/hendrych/Thesis.pdf, 2002.

34. **Makarov, Vadim.** *Quantum cryptography and quantum cryptanalysis.* Norwegian University of Science and Technology. Tesis doctor en Ingeniería, Marzo del 2007

35. **Capraro, Ivan.** *Advanced Techniques in Free Space Quantum Communication.* Universidad de Padova, Italia . Tesis para optar el grado de Doctor en Ingeniería de la Información. http://paduaresearch.cab unipd.it/615/1/phd_IvanCapraro.pdf, 2008.

36. **Henning Weier, Tobias Schmitt-Manderbach, Nadja Regner, Christian Kurtsiefer and Harald Weinfurter.** *Free space quantum key distribution Towards a real life application.* : Fortschr. Phys. 54, No. 8-10, 840- 845, 4 de agosto del 2006.

37 **Martínez, Jesús.** *Criptografía cuántica aplicada.* : Grupo de Investigación en Información y Computación Cuántica. Universidad Politécnica de Madrid., Abril del 2008.

38. **Landsberg.** *Optica Tomo II.* : Editorial MIR 1984, capitulo 23.

39. **J. G. Rarity, P. R. Tapster.** *Cryptographic receiver.* : European patent specification EP 0 722 640 B1, 1994.

40. **Ling, Alexander.** *Entangled State Preparation for Optical.* : Universidad de Singapur. Tesis para optar el grado de Doctor en Física, 2008.

41. **Garrison, J. C. y Chiao, R. Y.** *Quantum Optics.* : Oxford University Press, 2008.

42. **Lei Zhang, Jacob Barhen and Hua-Kuang Liu.** *Experimental and Theoretical aspects of quantum teleportation.* : Center for Engineering Science Advanced Research. Oak Ridge National Laboratory, 2000.

43. **Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger.** *Experimental quantum teleportation.* : Nature 390, 575-579, 1997.

44. **O'Brien, Jeremy L.** *Optical Quantum Computing.* : Science Vol 318, 11 de marzo del 2008.

45. **Dirac, P. A. M.** *The Principles Of Quantum Mechanics.* : Oxford University Press, 1958.

46. **Bennet, Charles H.** *Quantum Cryptography Using Any Two Nonortogonal States.* Physical Review Letters, Vol. 68, No 21, 25 de mayo de 1992.

47. **Ekert, Artur K.** *Quantum cryptography based on Bell's theorem.* : Phys. Rev. Lett. 67, 661 - 663, 1991.

48. **C.H. Bennett, G. Brassard, and N.D. Mermin.** *Quantum cryptography without bell's theorem.* . Phys. Rev. Lett. 68, pág 557-559, 1992.

49. **Fox, Mark.** *Quantum Optics,.* : Oxford University Press, 2006.

50. **Robert Davies, Jeremy Thorn, Matt Neel, Vinsunt Donato, Jeff Bergreen, Ashifi Gogo, Will Snyder, Matt Olmstead, Alex Carlson, Jesse Lord, Dave Branning and Enrique Galvez.** *Quantum Mechanics. Laboratory Manual.* : Mark Beck, 2008.

51. **Paul G. Kwiat, Edo Waks, Andrew G. White, Ian Appelbaum, and Philippe H. Eberhard.** *Ultra-bright source of polarization-entangled photons.* : Los Alamos National Laboratory and University of California, 22 de mayo de 1999.

52. **(CSIC), Consejo Superior de Investigaciones Científicas.** *Un experimento dirigido por el CSIC mejorará la tecnología para luchar contra el espionaje y la piratería informática.* : Universidad de Valencia, España. www.csic.es, 2 de junio del 2008.

53. **Optoelectronics, PerkinElmer.** *Avalanche photodiode. User Guide.* : PerkinElmer Inc. www.optoelectronics.perkinelmer .com, 2006.

54. **Negrevergne, T.S. Mahesh, C. A. Ryan, M. Ditty, F. Cyr-Racine, W. Power, N. Boulant, T. Havel, D.G. Cory and R. Laflamme.** *Benchmarking quantum control methods on a 12-qubit system.* : Universidad de Waterloo- Canada y MIT - USA, 2006.

55. **J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, J. E. Mooij.** *Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits.* . Nature 447, 836 - 839, 14 de junio del 2007.

56. **L. DiCarlo, J. M. Chow, J. M. Gambetta, Lev S. Bishop, B. R. Johnson, D. I., Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf.** *Demonstration of Two-Qubit Algorithms with a Superconducting Quantum Processor.* Departments of Physics and Applied Physics, Yale University, New Haven, 01 de mayo del 2009.

57. **Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood and Isaac L. Chuang.** *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.* : Nature Vol. 414, 20-27, diciembre del 2001.

58. **C. H. Holbrow, E. Galvez, and M. E. Parks.** *Photon quantum mechanics and beam splitters.* : Department of Physics and Astronomy, Colgate University, 2001.

59. **Vlatko Vedral, Adriano Barenco and Artur Ekert.** *Quantum Networks for Elementary Arithmetic Operations.* : University of Oxford, 1995.

60. **Sara Gasparoni, Jian-Wei Pan, Philip Walther, Terry Rudolph and Anton Zeilinger.** *Realization of a photonic CNOT gate sufficient for quantum computation.* Universidad de Wien, 2004.

61 **Alberto Politi, Jonathan C. F. Matthews and Jeremy L. O'Brienm.** *Shor's Quantum Factoring Algorithm on a Photonic Chip.* : Science,Vol. 325. N°. 5945, pag. 1221, 4 September 2009.

62. **Anthony N. Vamivakas, Bahaa E. A. Saleh, Alexander V. Sergienko, and Malvin C. Teich.** *Theory of spontaneous parametric down-conversion from photonic crystals.* · Quantum Imaging Laboratory and Boston University, 2004.

63 **Balet, Laurent.** *Investigation into the Coupling of Quantum Dots to Photonic Crystal Nanocavities at Telecommunication Wavelengths.* : École Polytechnique Fédérale De Lausanne, Suiza. Tesis de Doctor en Ciencias Físicas, 2009.