# SISTEMA DE TRANSMISIÓN SEGURA PUNTO A PUNTO Y MULTIPUNTO EN MEDIOS COMPARTIDOS.

por

Alfredo Adrián Ortega

EN CUMPLIMIENTO PARCIAL DE LOS
REQUISITOS PARA OPTAR AL GRADO DE
DOCTOR EN INFORMÁTICA

DEL

INSTITUTO TECNOLÓGICO DE BUENOS AIRES
BUENOS AIRES, ARGENTINA
15 DE OCTUBRE, 2015

INSTITUTO TECNOLÓGICO DE BUENOS AIRES

DEPARTAMENTO DE DOCTORADO

Los aquí suscriptos certifican que han asistido a la presentación oral de la Tesis "**Sistema de transmisión segura punto a punto y multipunto en medios compartidos.**" cuyo autor es **Alfredo Adrián Ortega** completando parcialmente, los requerimientos exigidos para la obtención del Título de **Doctor en Informática**.

Fecha: 15 de Octubre, 2015

Directores:

Dr. Ignacio Alvarez-Hamelin

Dr. Diego Grosz

Tribunal de Tesis:

Dra. Jurado

Dr. Jurado

Dr. Jurado

INSTITUTO TECNOLÓGICO DE BUENOS AIRES

Fecha: **15 de Octubre, 2015**

Autor: **Alfredo Adrián Ortega**

Título: **Sistema de transmisión segura punto a punto y multipunto en medios compartidos.**

Departamento: **Doctorado**

Título Académico: **Doctor en Informática** Convocatoria: **12** Año: **2015**

Por la presente se otorga permiso al Instituto Tecnológico de Buenos Aires (ITBA) para: (i) realizar copias de la presente Tesis y para almacenarla y/o conservarla en el formato, soporte o medio que la Universidad considere conveniente a su discreción y con propósitos no-comerciales; y, (ii) a brindar acceso público a la Tesis para fines académicos no lucrativos a los individuos e Instituciones que así lo soliciten (incluyendo, pero no limitado a la reproducción y comunicación al público no comercial de toda o parte de la Tesis, a través de su sitios o páginas Web o medios análogos que en el futuro se desarrollen).

A excepción de lo autorizado expresamente en el párrafo precedente, me reservo los demás derechos de publicación y, en consecuencia, ni la Tesis ni extractos de la misma podrán ser impresos o reproducidos de otro modo sin mi previo consentimiento otorgado por escrito.

Declaro que he obtenido la autorización para el uso de cualquier material protegido por las leyes de propiedad intelectual mencionado o incluido en la tesis (excepto pasajes cortos, transcripciones, citas o extractos que solo requieran ser referenciados o citados por escrito) y que el uso que se ha hecho de estos está expresamente reconocido por las leyes aplicables en la materia.

Finalmente, manifiesto que la presente autorización se firma en pleno conocimiento de la Política de Propiedad Intelectual del ITBA y, en forma específica, del Capítulo 2.3. referido a la titularidad de derechos de propiedad intelectual en el ITBA y/o, según el caso, a la existencia de licencias no exclusivas de uso académico o experimental por parte del ITBA de la Tesis o la obra o de las invenciones allí contenidas o derivadas de ella.

Hago entrega en este acto de un ejemplar de la Tesis en formato impreso y otro en formato electrónico.

Firma del Autor

# Índice general

# Resumen

En esta Tesis se presenta una técnica novedosa de transmisión de datos en redes del tipo difusión de manera criptográficamente segura utilizando técnicas de espectro expandido y corrección de errores. Específicamente, el esquema propuesto implementa la multiplexación aleatoria de la información transmitida por clientes que comparten un medio de transmisión. En particular, se demuestra un sistema capaz de crear múltiples Virtual Local Area Networks (VLANs), criptográficamente seguras, utilizando cualquier medio de transmisión que pueda ser modelado como un canal Z. Se muestran prototipos funcionales, sobre software para el caso de la transmisión a tasas de kpbs en un medio acústico, y utilizando Field-Programmable Gate Arrays (FPGAs) en el caso de la transmisión a tasas de Gbps en un medio óptico. En el primer caso, se demuestra una tasa de 1 kbps con 16 clientes transmitiendo información simultáneamente y hasta una distancia de 1,2 m y, en el segundo, una tasa de 5 Gbps con 128 clientes simultáneos y distancias de hasta 20 km, con bajas tasas de error. El trabajo aquí presentado busca aportar alternativas para la implementación de seguridad en capa física para redes de comunicación multiusuario.

# Abstract

In this Thesis we present an original implementation of cryptographically secure transmission in broadcast-type networks by means of expanded spectrum and error correction techniques. Specifically, the proposed scheme relies on the random multiplexing of the information sent by clients sharing a transmission medium. We demonstrate a system capable of creating multiple cryptographically-secure Virtual Local Area Networks (VLANs) operating over any transmission medium which renders itself to be modeled as a Z channel. Working prototypes of the proposed scheme are demonstrated: A 1 kbps rate wireless, acoustic, communication system implemented on software, supporting up to 16 clients 1.2 m apart, and a 5 Gbps communication system implemented on a Field-Programmable Gate Array (FPGA), supporting the simultaneous transmission of up to 128 clients, with a reach of 20 km and low bit error rates. The ideas developed in this Thesis seek to offer alternatives to the implementation of security in the physical layer in multiuser communication networks.

# Lista de Publicaciones

Lo reportado en las siguientes publicaciones conforma la base de la presente Tesis:

- **Altas velocidades de transferencia en fibra óptica utilizando FPGAs de bajo costo.** *A. A. Ortega, V. A. Bettachini, D.F. Grosz, J. I. Alvarez-Hamelin - Congreso de Microelect rónica Aplicada 2010 BsAs*

- **Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security** *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz, Advanced Photonics 2011 Congress - Access Networks and In-house Communications, OSA Technical Digest, Optical Society of America*

- **Hamming-weight minimisation coding for CDMA optical access networks with enhanced security** *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz - Future Generation Communication Technology (FGCT) 2012*

- **Encrypted CDMA Audio Network.** *A. A. Ortega, V. A. Bettachini, P. I. Fierens, J. I. Alvarez-Hamelin - Journal of Information Security - 2014*

- **Dispositivo y Método para Transmisión Segura de Datos sobre Canales Z Mediante CDMA (AR084155B1)** *José Ignacio ALVAREZ HAMELIN, Victor Alexis BETTACHINI y Alfredo ORTEGA. PCT, 12 2012. (Asignada)*

- **Dispositivo y método para transmisión segura de datos sobre canales Z mediante CDMA**, J.I. Alvarez-Hamelin, V.A. Bettachini, A.A. Ortega, PCT Internacional, N/Ref. PCT/IB2012/057003, 5 de diciembre, 2012.

- **Device and Method for the Secure Transmission of Data over Z-Channels Using CDMA**, J.I. Alvarez-Hamelin, V.A. Bettachini, A.A. Ortega, Presentación a la oficina de Patentes Europea P11104EPPC, 4 de Julio

del 2014.

# Reconocimientos

Esta Tesis esta dedicada a las personas que me alentaron constantemente y la hicieron posible: mis supervisores Dr. Jose Ignacio Alvarez Hamelin y Dr. Diego Grosz, los investigadores del laboratorio de Optoelectrónica del ITBA y a su director Dr. Pablo Fierens, a los expertos de nivel mundial (y próximamente inter-planetario) en seguridad informática Gerardo Richarte y Ariel Futoransky, y por supuesto, mi familia.

# Índice de figuras

# Capítulo 1

# Introducción

En esta Tesis se presenta una técnica novedosa de transmisión de datos en redes de tipo difusión, con énfasis en la privacidad, utilizando técnicas de espectro expandido.

Los sistemas de comunicación ópticos han hecho posible las comunicaciones modernas. Tecnologías como Internet están mayormente implementadas sobre una infraestructura óptica de comunicaciones de alta velocidad. La tasa de transmisión en enlaces individuales de la columna vertebral (*backbone*) de Internet ha evolucionado recientemente de 10 Gbps, 100 Gbps y hasta 400 Gbps [2] al momento de escribir este documento, utilizando técnicas tales como WDM (*wavelength division multiplexing, multiplexación por división de longitud de onda*) y modulación coherente [3], ambas tecnologías utilizadas para aumentar la tasa de transmisión de datos sobre la fibra óptica. Las redes de computadoras en general son redes de conmutación (*packet switching)*, donde un ruteador procesa electrónicamente grupos de bytes denominados "paquetes" y los retransmite a los nodos de destino, enviando cada paquete individual a la interfaz de red correcta (ver Fig. 1.1). Es un mecanismo eficiente en ancho de banda utilizado, pero requiere de una elevada cantidad de procesamiento.

Otro tipo de redes son las llamadas redes de difusión o *broadcast*, que poseen algunas ventajas con respecto a las redes de conmutación de paquetes, tales como un sistema de ruteo mucho más simple que puede ser totalmente óptico, pero también tienen desventajas, tales como la necesidad de compartir el ancho de banda y problemas de seguridad inherentes al enviar la información a todos los nodos de la red. De esto se desprende que las redes de difusión deben generalmente contar con algún mecanismo que ofrezca privacidad, o de lo contrario su uso se restringe a aplicaciones

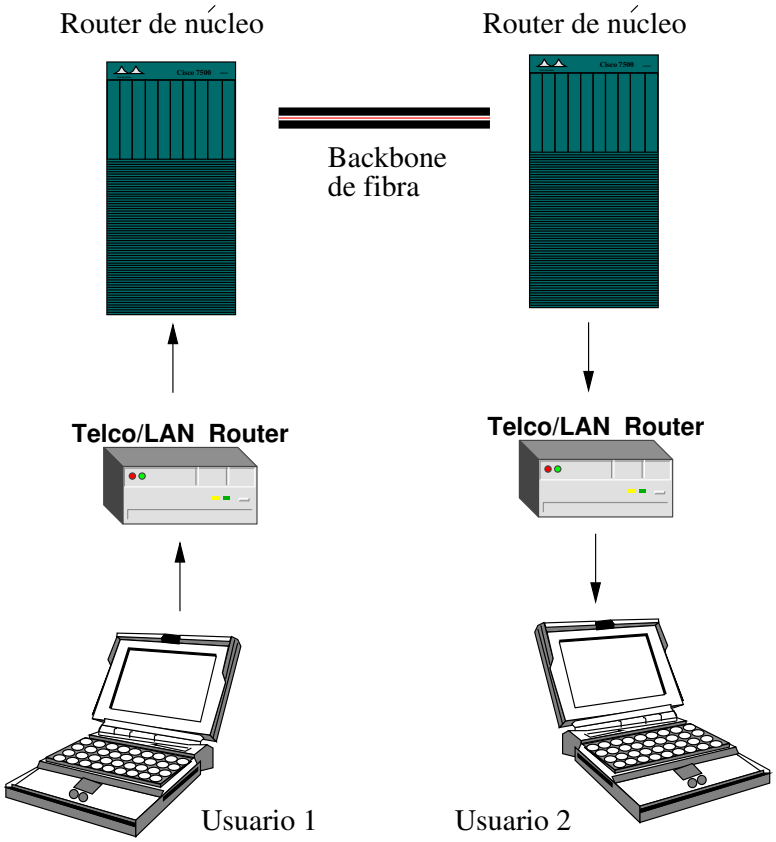



Figura 1.1: Diagrama esquemático del sistema de ruteo de Internet.

que, o bien no requieren de ningún tipo de privacidad, o la privacidad se logra utilizando protocolos de alto nivel. Es sobre este tipo de redes donde se centra el aporte de esta Tesis.

Las redes de difusión no están limitadas al medio óptico. Pueden utilizar el medio electromagnético (por ejemplo, ondas de radio) o acústico (modems). Las comunicaciones de radio, por ejemplo, pueden ser espiadas por cualquier atacante que tenga una simple antena. Fue este problema en las comunicaciones de radio lo que impulsó la invención de técnicas criptográficas avanzadas en la segunda guerra mundial. Las comunicaciones de tipo difusión resultaron ser ideales para coordinar acciones bélicas en la segunda guerra, donde un emisor central podía impartir órdenes a toda el ejército utilizando ondas de radio, con la condición obvia que únicamente aliados puedan participar de las comunicaciones. Esto motivó el desarrollo de los primeros dispositivos criptográficos tales como la máquina de Enigma [4], así como los primeros

ataques matemáticos a la criptografía [5].

En tiempos modernos, las comunicaciones de tipo difusión fueron en gran parte desplazadas con respecto a las redes de conmutación de paquetes, especialmente en redes digitales de comunicaciones tales como Internet. Sin embargo, existen nichos donde por motivos prácticos siguen siendo utilizadas redes de difusión casi exclusivamente, tales como la televisión y la telefonía satelital. Gran parte de la complejidad de estos sistemas se debe a los mecanismos de seguridad que deben implementar para prevenir fraudes y pérdida de privacidad [6].

Continuando con esta línea de investigación, los problemas de seguridad en las redes de difusión motivaron el diseño que utiliza un medio óptico o acústico donde la privacidad esté implementada en la capa física, sin requerir ningún tipo de soporte de software o del sistema operativo. El objetivo fue crear una VLAN *(Virtual Local Area Network, red local virtual)* donde cada cliente pueda realizar comunicaciones de datos privadas con cualquier otro, sin revelar ninguna información a los demás.

Esto apunta a fomentar el desarrollo de sistemas de FTTH (*Fiber to the Home*) sobre redes PON (*Passive Optical Network*) [7] donde un diseño de red de difusión óptica con seguridad a nivel físico permitiría utilizar componentes pasivos de muy bajo costo (ver Fig. 1.2). Si bien es sencillo realizar un enlace punto-a-punto, óptico o acústico, utilizando cualquier algoritmo de encriptación simétrica, la creación de una verdadera red, con múltiples clientes y canales punto-a-multipunto, no tiene una solución clara hasta el momento.

Luego de un período de exploración de posibles diseños y soluciones, se desarrolló un sistema de comunicaciones. Se calculó su eficiencia teóricamente y por medio de simulaciones, para finalmente proceder a su implementación como prototipo, primero sobre un medio acústico y finalmente sobre un medio óptico. En el medio acústico se utilizaron dispositivos informáticos comunes, tales como laptops y teléfonos celulares del tipo smartphone, utilizando los micrófonos y parlantes de los mismos para establecer una red VLAN acústica. Para la implementación sobre medio óptico se utilizó una placa de desarrollo FPGA, un dispositivo capaz de procesar las altas tasas de transferencia del medio óptico. Esta Tesis documenta las experiencias obtenidas en el diseño, implementación y medición del algoritmo implementado sobre varios

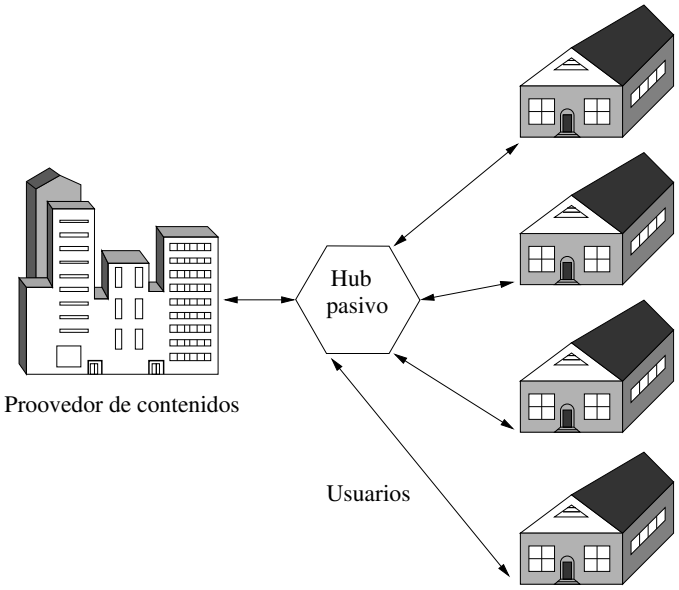



Figura 1.2: Sistema FTTH propuesto. Un proveedor de contenidos (Ej. Datos, TV, o telefonía, lo que se denomina "triple-play") utiliza un concentrador de muy bajo costo para conectarse, directamente, a los usuarios finales por medio de una conexión de fibra óptica.

dispositivos y medios diferentes.

## 1.1 Contribuciones

Se nombran las contribuciones que esta Tesis ha realizado a la comunidad, en la forma de artículos o patentes, acompañados de un breve resumen de los mismos:

**Altas velocidades de transferencia en fibra óptica utilizando FPGAs de bajo costo.** *A. A. Ortega, V. A. Bettachini, D.F. Grosz, J. I. Alvarez-Hamelin - Congreso de Microelectrónica Aplicada 2010 BsAs*: en este artículo se documenta una técnica para utilizar FPGAs (*Field Programmable Gate Array*) con transceptores ópticos normales, a mayor velocidad que la documentada. Utilizando los circuitos internos del transceptor independientes de los circuitos de la FPGA que lo contiene, es posible generar señales de pruebas de hasta 12 Gbps, con una longitud máxima de patrón de 11 bits individualmente controlables. Estos patrones de prueba tienen aplicaciones tanto para la caracterización de canales como para la experimentación con pulsos laser o eléctricos.

**Point-to-point and Point-to-multipoint CDMA Access Network with Enhanced Security** *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz, Advanced Photonics 2011 Congress - Access Networks and In-house CommunicationsAccess Networks and In-house Communications, OSA Technical Digest, Optical Society of America*: se presenta la primera versión de la red segura, funcionando sobre un medio de fibra óptica y con un aprovechamiento del medio del 13 %. Se propone una diseño de red segura en la capa física, utilizando la técnica de time-hopping CDMA, y logrando comunicaciones criptográficamente seguras punto-a-punto y punto-a-multipunto. Una implementación con topología en estrella es analizada, soportando hasta 128 usuarios situados hasta a 20 km de distancia del nodo central. Se utiliza el algoritmo LDPC (*Low Density Parity Check*) como parte del sistema de corrección de errores. Se demuestra la viabilidad del sistema mediante simulaciones numéricas.

**Hamming-weight minimisation coding for CDMA optical access networks with enhanced security** *A. A. Ortega, V. A. Bettachini, J. I. Alvarez-Hamelin, D.F. Grosz, Future Generation Communication Technology (FGCT), 2012*: este artículo se muestra un diseño similar al anterior, pero con una modificación en la pila de corrección de errores que eleva el aprovechamiento del medio al 33 %. Esto se logra eliminando la etapa de corrección LDPC y reemplazándola por una corrección de errores realizada directamente en el Bloom Filter encriptado, que es optimizado por el algoritmo de minimización de peso de Hamming. Utilizando un diseño en estrella, el sistema soporta 128 usuarios simultáneos situados hasta a 20 km de distancia del nodo central. Hay que destacar que estas características se cumplen utilizando un hub central pasivo. Utilizando un repetidor o hub central activo, las distancias pueden ser mayores.

**Encrypted CDMA Audio Network.** *A. A. Ortega, V. A. Bettachini, P. I. Fierens, y J. I. Alvarez-Hamelin - Journal of Information Security - 2014*: este artículo se centra en la implementación del protocolo sobre el medio acústico, ahondando en

la sincronización, implementación y mediciones sobre distintos dispositivos móviles, tales como celulares y laptops, demostrando que si bien la modulación necesaria para la creación de un canal Z tiene muy baja eficiencia espectral, es altamente compatible, resistente a interferencias y puede ser utilizada para transmitir de manera privada a distancias prácticas por la mayoría de los dispositivos testeados.

Fueron presentados los siguientes pedidos de patentes en oficinas de patentes nacionales (Argentina) (patente asignada) e internacionales (EU) (patente en trámite al momento de escritura de esta Tesis):

**DISPOSITIVO Y MÉTODO PARA TRANSMISIÓN SEGURA DE DATOS SOBRE CANALES Z MEDIANTE CDMA (AR084155B1)** *José Ignacio ALVAREZ HAMELIN, Victor Alexis BETTACHINI, and Alfredo ORTEGA. PCT, 12 2012. (Asignada)*

**Device and Method for the Secure Transmission of Data over Z-Channels Using CDMA (P11104EPPC)** *José Ignacio ALVAREZ HAMELIN, Victor Alexis BETTACHINI, and Alfredo ORTEGA. EPO, Julio 2014. (En trámite)*

## 1.2 Organización de esta Tesis

En el primer capítulo "Introducción" se presentan las motivaciones, contribuciones y algunas definiciones. Se describe en alto nivel la estructura de la Tesis.

En el segundo capítulo "Fundamentos y estado del arte" se presenta un resumen de todas las tecnologías utilizadas, así como las definiciones necesarias.

En el tercer capítulo "Sistema propuesto: teoría y simulaciones" se discuten las decisiones de diseño y se simula de manera numérica el sistema completo.

El cuarto capítulo "Resultados experimentales: medios de transmisión óptica y acústica" describe los detalles de implementación y mediciones en medios ópticos y acústicos. Se detalla el diseño de alto nivel de los generadores de trama en una FPGA para el protocolo en el medio óptico y la implementación en software que precisan los dispositivos móviles que utilizarán el medio acústico. Se detallan, también, los algoritmos de sincronización desarrollados, necesarios para las mediciones y para la creación de un prototipo funcional.

Finalmente, en el quinto capítulo “Conclusiones” se finaliza la Tesis presentando las conclusiones obtenidas, fruto de la investigación e implementación de los algoritmos y sistemas propuestos, y se sugieren posibles mejoras o aportes específicos a realizar en el futuro.

# Capítulo 2

# Fundamentos y estado del arte

En este capítulo se presentan las bases y fundamentos de las técnicas desarrolladas y utilizadas en esta Tesis. Primeramente, se da una breve explicación del concepto de códigos correctores de errores, continuando con los distintos algoritmos utilizados en la implementación. Luego, se define el concepto de espectro ensanchado, una técnica utilizada en comunicaciones pero implementada de un modo poco convencional en esta Tesis. Posteriormente, se definen los aspectos de seguridad a tener en cuenta al utilizar los algoritmos previamente mencionados, así como el el concepto de nivel de fuerza criptográfica y de cual es el objetivo a alcanzar con respecto a este último tema.

Para finalizar, en la sección de estado del arte se repasa el estado de las tecnologías y sistemas en uso actualmente, y se lo compara con el sistema descrito en esta Tesis.

## 2.1 Códigos correctores de errores

Para trasmitir información digital a través de un medio analógico, tal como una fibra óptica, las señales digitales originales deben convertirse en señales analógicas. Toda señal analógica que se transmite o almacena en un medio físico, invariablemente, sufre una degradación producto de las imperfecciones de los transductores, imperfecciones o limitaciones en la codificación, o ruido de diferentes tipos. Esta degradación puede ocurrir en cualquier módulo del sistema, o las interfaces entre los mismos, y generalmente es deseable que el sistema pueda reproducir los datos almacenados o transmitidos con la menor cantidad posible de errores. La diferencia entre la señal

transmitida y la recibida se suele modelar como ruido con una determinada distribución de potencia superpuesta a la señal codificada (ignorando efectos como atenuación y distorsiones). Algunos modelos de ruido, tal como el ruido aditivo gaussiano, son muy utilizados para modelar la interferencia producto de fuentes naturales como ruido térmico o para aproximar fuentes de ruido no lineales.

Al transmitir datos digitales sobre canales con ruido, aún asumiendo que las etapas moduladoras y demoduladoras sean capaces de reproducir los datos fielmente, el mensaje recibido $m_r$ sera distinto al mensaje original $m$, ya que la señal que recibe el demodulador sera una combinación de la señal original emitida con el ruido. La diferencia entre $m_r$ y $m$ se denomina "error de transmisión". Para aumentar la confiabilidad y reducir el error de transmisión se idearon códigos correctores/detectores de errores, con los que el receptor puede detectar un error y pedir una retransmisión, o bien corregir el error utilizando datos adicionales presentes en la señal. Los métodos de corrección de errores o "*channel coding*", generalmente funcionan aumentando la redundancia de la información, aumentando el tamaño del mensaje sin aumentar su entropía o cantidad de información [8].

Un método trivial de corrección de errores consiste en detectar cambios en el mensaje por medio de un código de detección, como puede ser una suma de verificación, el algoritmo CRC (*cyclic redundancy check*) o una función de hash [9], e iniciar el proceso de retransmisión del segmento o trama de datos afectada. Este simple método posee la desventaja de ser costoso, tanto en ancho de banda utilizado, como en el retraso de la transmisión. En enlaces de muy alta velocidad, las elevadas tasas de retransmisión hacen que este algoritmo sea sumamente ineficiente. Es por lo tanto deseable utilizar un algoritmo que pueda detectar y corregir errores basado solamente en información adicional transmitida, sin utilizar retransmisiones. Esta técnica se denomina *Forward Error Correction Codes*, o códigos FEC [8] de los cuales existen diferentes tipos de acuerdo con sus aplicaciones, rendimiento y parámetros. A continuación, se describen los algoritmos que fueron utilizados en el sistema propuesto en esta Tesis.

### 2.1.1 BCH/Reed Solomon

Los códigos BCH y Reed-Solomon [10] son usados ampliamente en la industria de comunicaciones y almacenamiento masivo por su bajo consumo de recursos computacionales y desempeño, desde el punto de vista de la proporción entre errores corregidos e información de paridad agregada. El algoritmo Reed-Solomon pertenece a una clase de códigos lineales denominados *maximum distance separable* (MDS ), que se consideran óptimos en esta relación. Estos códigos consisten en una representación de los datos basada en grupos algebraicos cíclicos. Esta familia de códigos fue introducida en 1959, pero es todavía utilizada en estándares de Ethernet de 10 Gbps, 100 Gbps y hasta 400 Gbps [11] debido a su robustez, bajo retraso y la existencia de algoritmos eficientes para la decodificación en un tiempo fijo.

### 2.1.2 LDPC

El esquema de corrección de errores llamado *Low Density Parity Check* (LDPC) o bien conocido como códigos de Gallager [12] es un caso notable: introducido en los años 60, fue olvidado debido a la alta capacidad de procesamiento y memoria requeridos, ya que para su implementación es necesario utilizar matrices de paridad de gran tamaño. Sin embargo, con los avances en hardware informático, este algoritmo se volvió una opción viable y actualmente es utilizado en sistemas modernos [13] debido a su simplicidad y gran capacidad de corrección de errores, en algunos casos, permitiendo alcanzar una capacidad de canal próxima al máximo teórico. Antes de ahondar en la descripción de este algoritmo debemos aclarar que, a pesar de ser utilizado para ciertos modelos durante la primera fase de la investigación, fue descartado en la versión final por un modelo más simple y con menos requerimientos de hardware que presenta una desempeño similar desde el punto de vista de corrección de errores.

LDPC es un código que se denomina *capacity approaching*, esto es, para un canal discreto sin memoria con un determinado nivel de ruido, la capacidad del canal definida como el límite máximo de la tasa de transmisión posible sin errores, puede estar cerca del límite teórico propuesto por Shannon [14]. El algoritmo se basa en un código lineal que utiliza una matriz de paridad $H$ grande y dispersa. Siendo un código lineal, una matriz de paridad tiene la propiedad de que todo codeword $x$ válido cumple con

$H * x = 0$.

Existen muchos métodos para construir la matriz de paridad; uno muy utilizado consiste simplemente en generarla aleatoriamente [12]. Otras maneras de generar la matriz son posibles y es un campo de investigación activo actualmente [15].

## 2.2 CDMA

La multiplexación por división de código, acceso múltiple por división de código o CDMA (del inglés, *Code Division Multiple Access*) es el nombre genérico de varias técnicas de comunicación basadas en el espectro expandido, con el fin de lograr multiplexación o control de acceso al medio. Se denomina espectro expandido a la utilización de mayor ancho de banda que el necesario para la transmisión correcta de los datos. Generalmente, se logra mediante la combinación de una señal señal de ensanchamiento o de pseudoruido, con la señal original, utilizando diferentes métodos.

Los orígenes de este algoritmo se remontan al año 1903, cuando Nicola Tesla patentó el concepto de *Frequency hopping* o salto en frecuencia, uno de los métodos de CDMA utilizados actualmente.

Estas técnicas apuntan a conferir las siguientes propiedades al sistema de comunicaciones:

1. Resistencia contra ruido e interferencias: como una fuente de ruido generalmente sólo afecta una region del espectro, la mayor parte de la señal no se verá interferida, pudiéndose recuperar el resto de la información mediante técnicas de corrección de errores.

2. Privacidad: si un atacante no conoce la secuencia que se utilizó para expandir el espectro de la señal original (secuencia creada, por ejemplo, por un generador de números pseudoaleatorios o PRBS, ver 2.3), se dificulta o imposibilita diferenciar la señal expandida del ruido.

3. Capacidad de acceso múltiple: varios usuarios pueden transmitir utilizando el mismo medio y la misma área espectral mientras utilicen diferentes códigos.

Existen varios métodos de CDMA (ver Fig. 2.1 para una representación gráfica), entre ellos:

1. *Direct-Sequence Spread Spectrum* (DSSS): se expande la señal combinándola con un código de pseudoruido o señal de ensanchamiento, mediante la operación lógica XOR, o mediante desplazamientos de fase. Este método es el utilizado en WiFi y WiMAX, redes 3G de celulares [16], el sistema GPS [17], etc.

2. *Frequency-Hopping Spread Spectrum* (FHSS): la señal de ensanchamiento o pseudoruido es en este caso utilizada para variar la frecuencia portadora o canal de la señal original. Este método es empleado, por ejemplo, en el sistema BlueTooth de comunicación digital. En este caso se utiliza una variación llamada *Adaptive Frequency Hopping*, un método para evitar frecuencias con mucha interferencia [18].

3. *Time-Hopping Spread Spectrum*: en este método, también llamado modulación por posición de pulso, la señal de datos no se transmite todo el tiempo sino que se divide en pulsos de transmisión, que sufren de un retraso que depende de la señal de ensanchamiento o pseudoruido. Actualmente, esta técnica no es tan utilizada como las anteriores, aunque se estudiará detenidamente en nuestro caso ya que fue el método seleccionado.

## 2.3 Códigos de generación de pseudoruido

El código CDMA requiere de una secuencia de pseudoruido, también denominada pseudoaleatoria, para modular la señal original. Existen muchos algoritmos para generar este tipo de secuencias, dependiendo de las características deseadas. Es posible utilizar una secuencia corta predecible si la aplicación no requiere de privacidad. Por ejemplo, el protocolo WiFi 802.11b multiplica cada bit por una secuencia de sólo 11 bits, denominada secuencia de Barker [19].

Si fuera necesario que la comunicación sea privada, es deseable que la secuencia pseudoaleatoria posea las siguientes características:

1. Debe ser sólo conocida por las entidades comunicantes.

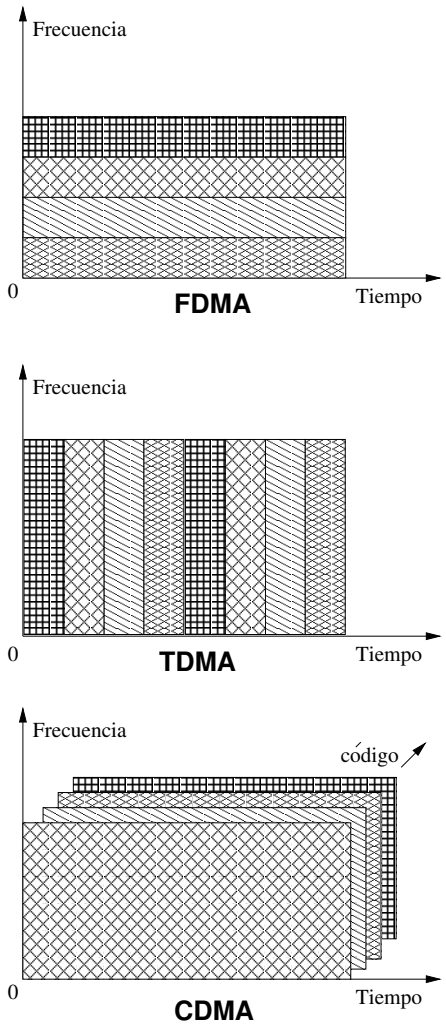



Figura 2.1: Comparación gráfica entre las separaciones de canal en TDMA (*Time Division Multiple Access*), FDMA (*Frequency Division Multiple Access*) y CDMA (*Code Division Multiple Access*)

2. No se debe repetir la secuencia, para que la misma no se pueda deducir por simple observación.

3. Ninguna parte de la secuencia debe poder estimarse por una entidad externa a las comunicantes sin conocer los parámetros de generación.

Estas características pueden lograrse utilizando un algoritmo denominado *generador pseudoaleatorio* (PRBS, según la sigla en inglés), que genera la secuencia basado en un parámetro de inicialización o semilla, siendo capaz de generar un flujo de

números aparentemente aleatorio pero, en realidad, totalmente determinístico. Adicionalmente, un generador que cumple con el punto 3) se denomina *criptográficamente seguro*, ya que es apto para su uso en criptografía. Es necesario que los nodos que participen de toda comunicación privada puedan generar exactamente la misma secuencia, por lo que deberán compartir la *semilla* del PRBS.

Existen muchos métodos o algoritmos para generar flujos de números pseudoaleatorios. Un parámetro importante es la cantidad de bits que el generador es capaz de producir antes de que se repita la secuencia o período. Este parámetro es denominado el *período del generador*, y en aplicaciones criptográficas es deseable que sea lo mayor posible. Sin embargo, el hecho de tener un período largo no es suficiente para que el generador pseudoaleatorio pueda ser utilizado en aplicaciones criptográficas. Podemos citar el caso del algoritmo denominado Mersenne-twister [20], cuya aplicación más popular tiene un periodo de $2^{19937}-1$; sin embargo existen métodos para predecir la secuencia sin conocer la semilla [21], por lo que no es apto para su uso en aplicaciones seguras. Otras características deseables en un generador PRBS son, su baja complejidad, bajo consumo de recursos y alta velocidad de generación. Un generador PRBS muy popular utilizado en implementaciones de software es el denominado *generador congruencial lineal*, un algoritmo extremadamente simple que sólo precisa de dos operaciones: una multiplicación y una suma, siendo utilizado en aplicaciones de estadística y software [22].

### 2.3.1 Generadores criptográficamente seguros

Los ejemplos mencionados en la sección anterior carecen de una característica fundamental requerida en el sistema propuesto: que no se puedan predecir sin conocer absolutamente todos los parámetros del generador. Esta simple característica no es en realidad trivial ya que existen técnicas para inferir datos acerca del generador PRBS [21], que supondría una falla en la seguridad de un sistema basado en dicho generador. Los algoritmos que no sufren de este problema son llamados *generadores criptográficamente seguros* o CS-PRNG, por su sigla en inglés. Como ejemplo, podemos nombrar a los generadores del tipo *shrinking* [23]. Constantemente surgen nuevos ataques a

generadores utilizados por la industria, tales como el generador utilizado por el algoritmo RC4 [24], por lo que es imprescindible estar actualizado en los avances de investigación criptográfica al diseñar un sistema seguro. En el caso de RC4, el mismo creador (Ron Rivest) ha desarrollado recientemente un reemplazo corrigiendo varias vulnerabilidades y manteniendo las características deseables del mismo, denominado *Spritz* [25].

Los generadores pseudoaleatorios suelen ser costosos computacionalmente, una de las razones por la cual las transmisiones de muy alta velocidad no suelen ser encriptadas, aunque avances en hardware con aceleradores específicos [26] están logrando que la implementación de enlaces criptográficos sea cada vez mas común.

## 2.4 Seguridad

Se propone utilizar un sistema de espectro expandido con el objetivo principal de lograr la privacidad del canal, al nivel físico, en sistemas de comunicación ópticos y acústicos. Para este propósito, se fijaron los siguientes parámetros de seguridad que debe cumplir la implementación:

- El sistema debe proveer confidencialidad, integridad y privacidad de los datos.
- El sistema debe ser seguro, sin importar la cantidad de clientes existentes o la naturaleza de los datos que se transmiten.
- Un atacante no debe poder identificar los datos de un cliente, aunque controle todos los nodos restantes de la red. Es decir, el sistema debe garantizar privacidad ante un ataque coordinado donde la mayoría de los nodos de la red son maliciosos. Esto imposibilita el uso de ciertos algoritmos (como códigos de Gold [27]) donde es posible inferir la secuencia de cualquier nodo a partir del conocimiento de la secuencia de la mayoría de ellos.

Con estos parámetros se buscó el algoritmo CDMA adecuado. Si bien la implementación en un sistema acústico no presenta grandes limitaciones en la técnica utilizada debido a los bajos recursos computacionales necesarios, las características de un sistema óptico de alta velocidad hacen muy complejo el hardware requerido para lograr

DSS-CDMA o *frequency hopping*. Sin embargo, implementar time hopping no presenta costo ni dificultad adicional, por lo cual fue el seleccionado en el diseño final.

Como se explicó en 2.2, el algoritmo de time hopping consiste en dividir el tiempo en segmentos denominados *tramas*, compuestos de *slots* o casilleros, y modular el casillero asignado a cada nodo por medio del generador PRBS. De esta manera puede verse como la señal efectúa saltos o "hops" en el tiempo a medida que es transmitida en diferentes casilleros.

Una propiedad deseable es que los códigos generadores de todos los canales es que sean ortogonales entre sí, es decir, que la salida de dos o más generadores nunca coincida al mismo tiempo. Esto es debido a que la salida de los generadores determina la posición del casillero dentro de la trama, entonces, si dos o más posiciones coinciden, los clientes intentarán utilizar el mismo casillero para transmitir sus datos y se producirá una colisión entre ellos. Esto no sucedería nunca con códigos totalmente ortogonales entre sí. Sin embargo, para lograr esta característica es necesario compartir algún tipo de información entre todos los clientes, lo que debilita la seguridad del sistema. Por ejemplo, códigos existentes llamados *Gold codes* [27] permiten la generación de múltiples secuencias con baja correlación cruzada, y son utilizados para coordinar dispositivos que comparten el medio, ya que garantizan la ausencia de colisiones. Sin embargo, desde el punto de vista de la seguridad, estos códigos son trivialmente vulnerados. Por ejemplo, en un esquema donde un atacante controla todos los canales menos uno, el atacante podría simplemente dejar de transmitir y revelar la secuencia utilizada por la víctima, que forzosamente estará utilizando el canal restante.

Por este motivo se decidió utilizar una codificación trivial: seleccionar el casillero de acuerdo a una secuencia criptográficamente segura estándar, totalmente independiente de la de los otros canales. Este método causará colisiones entre los casilleros de transmisión, que aumentan con el número de clientes activos. Sin embargo, estas colisiones pueden ser corregidas mediante codificación FEC adicional, lográndose asá una utilización del canal próxima al máximo teórico, como se demuestra en la sección siguiente. De hecho, es en esta codificación adicional donde reside el principal aporte de esta Tesis.

## 2.5 Parámetro de seguridad

Para el análisis de complejidad de un sistema criptográfico se suele utilizar un parámetro variable que mide el tamaño del problema y representa a la vez los requerimientos del algoritmo criptográfico tanto como la probabilidad de un adversario de romper la seguridad en el sistema [28]. Este es el llamado *parámetro de seguridad*, que suele estar relacionado, por ejemplo, con el largo de clave. Este parámetro puede tomar valores arbitrariamente grandes. Además, la definición de seguridad depende de la tarea que el adversario trata de realizar y de la información acerca del esquema criptográfico disponible. Se suele especificar un valor en el cual la cantidad de cálculos necesarios por el atacante se presumen irrealizables, y en base a este valor se deberá seleccionar el parámetro de seguridad. Según la tesis de Cobham[29], el algoritmo del atacante se considera eficiente si esta limitado en tiempo polinomial sobra la longitud de la entrada (el parámetro de seguridad en este caso). En el caso que el atacante sólo pueda utilizar un algoritmo no-polinomial con respecto al parámetro de seguridad del sistema, el ataque se considera inviable. Nótese que el algoritmo criptográfico en sí mismo debe ser eficiente.

Finalmente, se debe fijar un límite debajo del cuál la probabilidad de un ataque efectivo es despreciable. El contrato criptográfico estándar trata a la probabilidad de ataque exitoso como despreciable si no excede $\frac{1}{p(n)}$ para un polinomio $p$ y el parámetro de seguridad $n$[28].

Aceptadas estas definiciones, para probar que un algoritmo criptográfico es seguro basta con probar que la imposibilidad de un algoritmo polinomial que realize la tarea del adversario.

De todas maneras, el estado actual de la teoría de complejidad no permite justificar un limite inferior de un problema como super-polinomial ($P = NP$?) por lo que la mayoría de las pruebas en el mundo de la seguridad están basadas en presunciones. Por lo tanto, la investigación se concentra usualmente en buscar las condiciones suficientes más débiles (o necesarios y suficientes) para la existencia de un esquema seguro. Las presunciones son usualmente generales, basadas en la teoría de la complejidad ó en la intratabilidad de ciertos problemas en la teoría de números.

### 2.5.1 Consideraciones de seguridad y fuerza de cifrado

En la seguridad de la información existen varios aspectos que deben tenerse en cuenta. Los más importantes son: confidencialidad, integridad, y disponibilidad (también denominados *The CIA triad* [30] por sus siglas en inglés). Pero no son los únicos, ya que la autenticación es otro aspecto fundamental. El esquema presentado en esta Tesis utiliza la técnica de CDMA para proveer confidencialidad, confiabilidad e integridad entre dos o mas partes y es equivalente a un esquema de clave simétrica, donde la clave compartida es utilizada para inicializar la semilla del algoritmo generador de PRBS. Aspectos adicionales, tales como la autenticación, pueden ser implementados luego utilizando protocolos de alto nivel [31]. El sistema propuesto fue específicamente diseñado tomando en consideración los ataques del tipo mencionados en la Ref. [32]. En dicha referencia se muestra que la seguridad no está debidamente resguardada en las versiones actuales de O-CDMA: la captura de sólo 100 bits por parte de un atacante puede reducir la relación señal a ruido requerida para romper el código a sólo 12dB. Como la seguridad del sistema es dependiente de su algoritmo generador de PRBS, se debe poner especial cuidado en la selección e implementación del mismo; debe ser un algoritmo generador de números aleatorios para usos en criptografía, es decir, criptográficamente seguro (CS-PRBS). Existen muchos algoritmos que cumplen con estos requisitos; el CS-PRBS utilizado en esta Tesis es el *self-shrinking generator* [33], pero puede utilizarse cualquier otro e incluso usar diferentes algoritmos para cada cliente, con la condición que dos clientes que deseen comunicarse deben utilizar el mismo algoritmo con los mismos parámetros y claves. Como en el caso de otros algoritmos de clave simétrica, la clave secreta debe distribuirse previamente utilizando un canal seguro [9].

Existe una vulnerabilidad adicional inherente a sistemas ópticos dispuestos como una red en estrella, tal como es el diseño propuesto en esta Tesis: los algoritmos de CDMA dependen de la interferencia para ofrecer confidencialidad. Sin embargo, en un sistema óptico con topología en estrella, existen secciones donde hay poca o ninguna interferencia. Un ejemplo, en el caso de la implementación óptica, sucede en el punto donde la red se conecta al nodo cliente, donde la señal de entrada, luego de atravesar varios kilómetros de fibra óptica, es de menor amplitud que la señal de

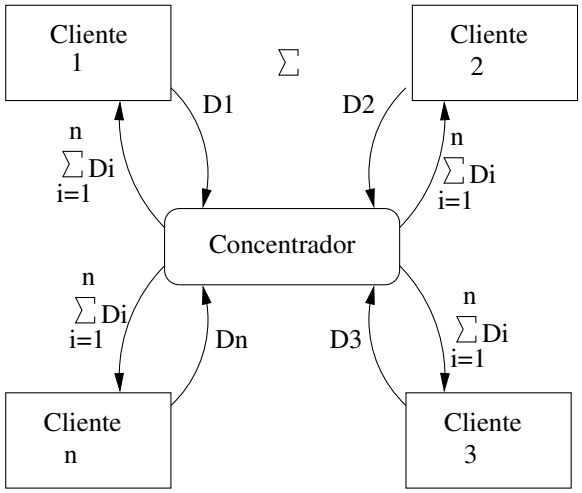



Figura 2.2: Esquema del concentrador central donde se observa que el flujo de datos de retorno es siempre la sumatoria de todos los datos de entrada.

salida. De esta manera es trivial diferencial la señal de salida con respecto al ruido de las demás transmisiones. Esta y otras vulnerabilidades fueron subsanadas en el diseño final mediante ajustes en la codificación.

Otra característica del algoritmo de encriptación propuesto es que no modifica el peso de Hamming del flujo de bits original: Se define al peso de Hamming de un símbolo como la cantidad de bits con valor "1" en el mismo. Muchos algoritmos de cifrado de flujo o *stream* se basan en la operación de XOR (el caso del algoritmo RC4), o bien una combinación de sustituir/transponer los datos antes de la transmisión (el caso de los algoritmos AES y DES), o transformaciones más complejas (caso RSA o algoritmos de curvas elípticas), ver Ref. [9]. Sin embargo, todas estas técnicas (con la excepción de códigos puramente permutativos) necesariamente modifican el peso de Hamming de cada símbolo. Como el algoritmo propuesto se basa en CDMA del tipo *time hopping*, efectivamente se encriptan los símbolos de entrada mientras que se mantiene inalterado el peso de Hamming en los datos de salida, una propiedad útil para ciertas codificaciones utilizadas posteriormente.

Podría argumentarse que el sistema es similar al esquema *Time Division Multiple Access* (TDMA, ver Fig. 2.1) donde también se divide el tiempo en tramas y casilleros. Pero en contraste con TDMA, en el esquema propuesto el atacante necesita interceptar cada una de las fibras ópticas para identificar a cada usuario, ya que no

es posible identificar exactamente el casillero de transmisión luego de pasar por el concentrador central. Por último, aún si el atacante pudiera identificar los datos, no podría descifrarlos sin poseer la clave correcta, ya que estos están desordenados por el time hopping y tienen normalizado el peso de Hamming.

## 2.6 Estado del Arte

A continuación se repasan las tecnologías disponibles actualmente para realizar encriptación sobre fibra óptica a altas velocidades y se mencionan otros tipos de redes con esquemas similares al propuesto.

### 2.6.1 Criptografía clásica

Las comunicaciones ópticas pueden utilizar algoritmos de criptografía clásicos, tales como encriptación de clave simétrica y asimétrica. La única dificultad consiste en que el procesamiento de datos debe ser lo suficientemente rápido para poder aplicarse al enlace de alta velocidad, lo que implica altos costos y procesadores con un alto consumo de energía, aún cuando el tiempo de procesamiento pueda reducirse arbitrariamente utilizando procesamiento en paralelo [11].

Actualmente, un dispositivo muy utilizado capaz de realizar criptografía a alta velocidad sobre fibra óptica es la FPGA, la cual, con la correcta paralelización del procesamiento de datos, puede alcanzar la velocidad máxima permitida por sus transceptores (por ejemplo, 400 Gbps [34]).

### 2.6.2 Criptografía puramente óptica

Un campo de investigación activo en la actualidad es el de la criptografía puramente óptica. La eliminación de las etapas electrónicas y la conversión electro óptica de los datos para su procesamiento tiene muchas ventajas, principalmente en la velocidad y la potencia consumida por el sistema. La dificultad principal de este método consiste en lograr una fuerza de cifrado adecuada, y en la implementación de los algoritmos necesarios utilizando solamente componentes ópticos. Podemos mencionar algunos resultados publicados tales como los avances en la creación de compuertas lógicas

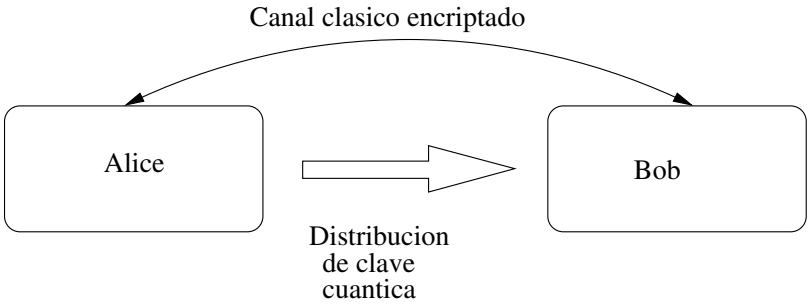



Figura 2.3: Esquema típico del método de distribución cuántica de claves.

puramente ópticas [35], o la utilización de señales caóticas para transmisión [36]. Debido a su novedad, no existen implementaciones prácticas de esta tecnología que estén siendo utilizadas en la industria al momento de la escritura de esta Tesis.

### 2.6.3 Encriptación cuántica

Una solución muy interesante a varios problemas criptográficos son las llamadas técnicas de criptografía cuántica, donde se aprovechan fenómenos de mecánica cuántica para lograr seguridad en las comunicaciones digitales. En estos sistemas, se codifica la información en estados cuánticos o *qubits*, en lugar de los bits, comúnmente utilizados para codificar datos en comunicaciones clásicas. Generalmente, se utilizan fotones para crear y medir dichos estados cuánticos, por lo que el medio de transmisión suele ser la fibra óptica, aunque es también es posible utilizar el aire como medio [37]. Uno de los problemas criptográficos resueltos utilizando mecánica cuántica es el de la distribución segura de claves. Algoritmos maduros de distribución cuántica de claves (Quantum key distribution [38]) actualmente son utilizados por la industria y cuentan con implementaciones comerciales e instalaciones a nivel metropolitano [39].

Dependiendo de la propiedad física aprovechada, los sistemas cuánticos pueden dividirse en dos categorías:

1. Sistemas basados en mediciones de variables físicas, en los que, a diferencia de lo que ocurren en la física clásica, la medición de un parámetro físico afecta el estado cuántico. Este fenómeno es utilizado para detectar cualquier interceptación de los datos, que necesariamente deberá realizar una medición sobre los mismos. Por ejemplo, un parámetro comúnmente seleccionado para codificar la

información es la polarización del fotón [40].

2. Sistemas basados en el entrelazamiento cuántico (*quantum entanglement*) [41], donde los estados cuánticos de dos o más elementos quedan unidos de forma que deben ser descritos mediante un estado cuántico combinado, y no como objetos individuales. Esto causa que la medición en uno de los objetos afecte a los otros (*acción a distancia*), y de esta manera puede detectarse cualquier interceptación.

En ambos casos, la seguridad se logra detectando una posible interceptación, en lugar de prevenir el acceso a los datos.

Generalmente, se utilizan varios canales sobre una fibra óptica, unos llamados "canales cuánticos" utilizados solamente para la distribución de claves, y otros "canales clásicos" donde se utiliza criptografía clásica (ver esquema en la figura 2.3). Por este motivo, muchos algoritmos de criptografía cuántica se denominan algoritmos de *quantum key distribution* (QKD).

Vale mencionar que la distribución segura de claves también puede realizarse utilizando un canal de comunicaciones clásico por medio de algoritmos matemáticos tales como Diffie-Hellman [42] o bien mediante la utilización de esquemas de clave pública [43].

Resumiendo, la seguridad de los sistemas de criptografía cuántica se basa en las bases de la mecánica cuántica, en contraste con los sistemas de criptografía tradicional que se basan en la complejidad computacional de ciertas funciones matemáticas [43]. Sin embargo, vulnerabilidades y fallas en la implementación siempre afectarán la seguridad de ambos tipos de sistemas [44].

### 2.6.4 Corrección de errores en canales asimétricos

Se denominan códigos de corrección de errores asimétricos o unidireccionales, a todo código de corrección especializado en canales de comunicaciones cuya probabilidad de error no se aplica simétricamente a todos los símbolos. Un caso sencillo, es por ejemplo, el del llamado canal Z, un canal binario (símbolos "1" y "0") pero cuyos errores sólo pueden afectar a uno de los símbolos, como podría suceder en un sistema

donde al transmitir el símbolo “0” un error provoque la recepción de un símbolo “1”, pero donde lo contrario no es posible. En la figura 3.5 se observa el diagrama de probabilidades del canal binario asimétrico o canal Z. En la sección 3.3.2 se desarrolla el límite de capacidad del canal Z.

Recientemente, surgió interés en el campo de la corrección de errores de canales asimétricos, debido a la utilidad de estos algoritmos en sistemas de almacenamiento digitales [45]. Sin embargo, el número de artículos publicados sobre el tema sigue siendo mucho menor en comparación con las publicaciones acerca de códigos de corrección para canales convencionales. Como ejemplo de códigos unidireccionales podemos citar los códigos de Berger [46] y códigos de Gallager o LDPC unidireccionales [47].

### 2.6.5 Sistemas de comunicación óptica

Existen muchos esquemas de distribución óptica en redes urbanas basados en redes ópticas pasivas, tales como APON [48] y sus derivados BPON/EPON, utilizados por millones de usuarios en la actualidad [49]. Sin embargo, el sistema que más se aproxima al descrito en esta Tesis es el *Secure Passive Optical Network* (SPON). En los SPONs [50], se agrega una capa de seguridad clásica por sobre un protocolo de comunicaciones preexistente como *Gigabit Passive Optical Network* (GPON).

Sistemas académicos se basan en encriptación puramente óptica tal como la descrita en 2.6.2 (Ver [51]). Algunas implementaciones proveen la misma funcionalidad que el sistema descrito en esta Tesis, tale como [52] aunque se diferencian en el tipo de CDMA utilizado y la topología de la red óptica.

### 2.6.6 Encriptación de comunicaciones acústicas

En esta Tesis se aborda el problema de la encriptación de un canal acústico multi usuario. En general, los sistemas de seguridad aplicadas a las comunicaciones acústicas han sido siempre en forma de capas adicionales de alto nivel funcionando por sobre las capas físicas [53]. Debido al poco ancho de banda disponible en el espectro de audio ($< 100Khz$), las comunicaciones acústicas tienen una tasa de transmisión reducida y es suficiente utilizar un CPU para todo proceso criptográfico. Existen ejemplos de modems acústicos comerciales capaces de encriptar su enlace [54], y recientemente

se han publicado esquemas en los que se utilizan algoritmos con una muy alta sensibilidad a condiciones iniciales, denominados algoritmos caóticos [55], para crear un sistema criptográfico sobre canales acústicos [56].

# Capítulo 3

# Sistema propuesto: teoría y simulaciones

Se propone un sistema de comunicaciones punto a punto y punto a multipunto sobre medios compartidos, o también llamados medios de *broadcast*. En la figura 3.1 se detalla la estructura de alto nivel del sistema, que en la versión óptica (ver Fig. 3.10) equivale a una red de tipo estrella con un concentrador/amplificador central. Utilizando diferentes medios de transmisión, esta configuración puede cambiar (por ejemplo, puede no ser necesaria la etapa de amplificación). Al ser un sistema de tipo time hopping CDMA 2.2, cada cliente puede utilizar el medio por un intervalo determinado de tiempo denominado *slot* o casillero. Esto permite utilizar el medio para múltiples clientes asignando a cada uno un casillero diferente. A diferencia de un sistema TDMA estándar, donde el casillero es asignado a cada cliente de manera periódica, en el sistema propuesto el casillero se asigna mediante un algoritmo CS-PRNG 2.3.1. Esto tiene dos efectos fundamentales:

- Un atacante no puede predecir la posición en donde un cliente en particular transmite los datos. En particular, si el tamaño del casillero se reduce al mínimo de un solo bit, el atacante no puede inferir ninguna información acerca de los datos transmitidos sin conocer los parámetros del algoritmo CS-PRNG.

- Existirá una inevitable interferencia entre los clientes, lo que requiere la utilización de algoritmos de corrección de errores.

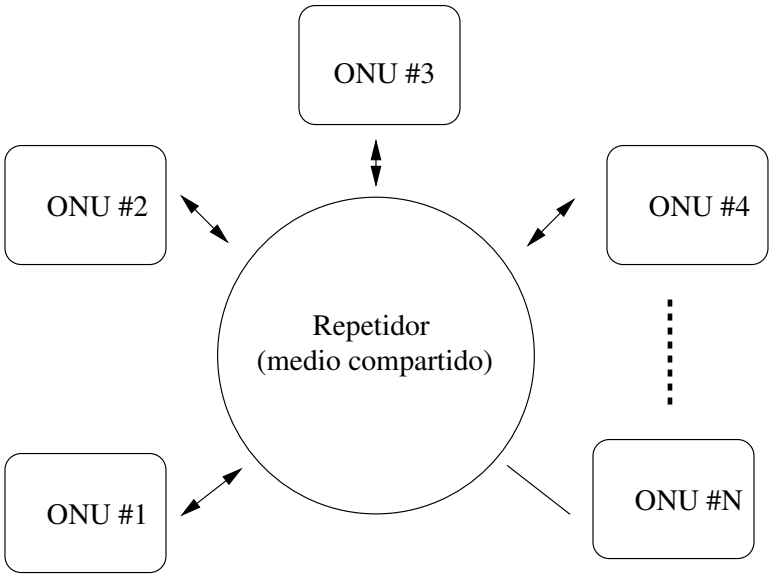



Figura 3.1: Estructura de alto nivel del sistema propuesto, donde un repetidor central distribuye el tráfico a múltiples *optical network units* (ONUs).

Como se describe en la sección 2.3.1, existen varios algoritmos CS-PRNG estandarizados [57]. Esta Tesis no ahonda sobre el tema y nos limitaremos a indicar que puede seleccionarse cualquiera algoritmo utilizado por la industria que no posea ninguna vulnerabilidad conocida. Otra característica que debe maximizar el algoritmo seleccionado es la cantidad de bits pseudoaleatorios generados por ciclo de reloj, ya que al ser utilizados para seleccionar la posición de cada bit en una trama de largo $M$, se necesitarán generar como mínimo $\log_2(M)$ bits aleatorios por cada bit de datos[1], por lo que, en general, la velocidad del PRNG afectará directamente la velocidad total de codificación y decodificación del sistema.

Un aporte importante de esta Tesis es el desarrollo de un método de corrección de errores adaptados al medio de transmisión, aprovechando las características del canal para recuperar información con una elevada cantidad de interferencia, producida por el método aleatorio de selección de casillero de transmisión.

La pila de codificación se detalla en la figura 3.2 donde puede verse su diseño convencional, excepto que en la última etapa de corrección de errores se aplica el algoritmo de filtros de Bloom, que aprovecha la característica de error asimétrico del

[1]Esta cantidad es tal debido a para codificar una posición dentro de $M$ posibles valores, se necesitan $\log_2(M)$ bits.

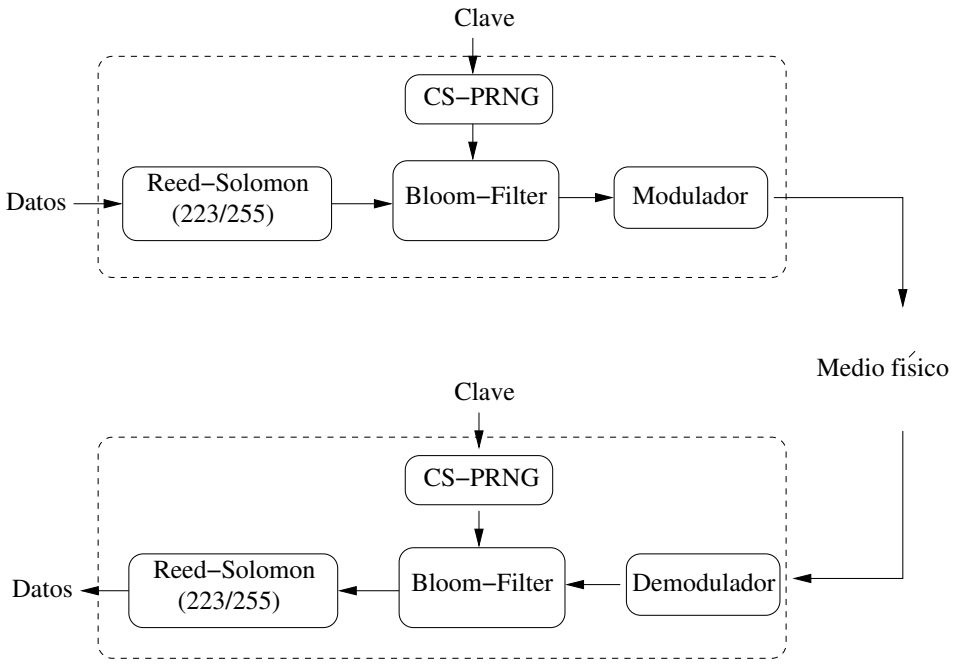



Figura 3.2: Diagrama esquemático del sistema de comunicaciones.

canal Z para una corrección adicional.

## 3.1 Códigos correctores de errores

La selección del código corrector de errores debe ser guiada por los parámetros del sistema, teniendo en cuenta que al operar en enlaces con tasas de transmisión elevadas, una de las limitaciones más importantes es la velocidad de procesamiento de datos del sistema.

En nuestro caso, se utilizó una típica estructura de dos códigos de corrección, uno denominado código exterior (*outer code*), y el segundo denominado código interior (*inner code*). La idea de utilizar dos códigos distintos es la de encadenar ambos algoritmos en serie para aprovechar las virtudes de dos tipos de corrección. Estos algoritmos se denominan códigos concatenados [58]. El motivo de utilizar códigos concatenados es que ciertos tipos de códigos tales como LDPC o códigos Turbo se caracterizan por poseer un piso de error elevado, que es un fenómeno donde el código pierde efectividad con relaciones señal/ruido elevadas [59]. Es para evitar esta pérdida de efectividad que se utiliza un segundo código corrector concatenado al primero,

denominado código interior, que si bien no es tan efectivo con bajas relaciones de señal/ruido como el código exterior, es efectivo con señales de bajo ruido, haciendo que el sistema sea eficiente en cualquier condición.

Un parámetro importante en estos algoritmos es el retraso de codificación o latencia, es decir, la cantidad de tiempo (medida usualmente en ciclos de reloj del procesador) que demora un bit entrante a la etapa de corrección en ser procesado y salir de la misma, luego de la aplicación de la corrección de errores. Esta latencia es variable según el algoritmo. Algunos algoritmos con una latencia importante no son óptimos para utilizar en aplicaciones de bajo ancho de banda que precisan de retransmisiones o confirmaciones de los datos, ya que a cada confirmación debe sumarse también este retraso, y esto suele resultar en una disminución apreciable de la velocidad de las comunicaciones. A continuación se detalla el algoritmo de corrección seleccionado.

### 3.1.1 Códigos de corrección Reed-Solomon

Como código interior se seleccionó el algoritmo Reed-Solomon, un código de bloque con alta efectividad en relaciones de señal/ruido bajas. La cantidad de paridad agregada por el algoritmo, y por lo tanto, la potencia de corrección, puede ajustarse a cada aplicación, sin embargo, en computadoras digitales binarias suelen tener registros cuyo largo es múltiplo de 8 bits, por lo que es eficiente utilizar 8 bits como tamaño de símbolo en Reed-Solomon. Debido a esto, un código muy utilizado es aquel que posee un tamaño de bloque de 255 bytes y 223 bytes de datos, con 32 bytes de paridad. Estos parámetros logran que el código pueda detectar hasta 32 errores de byte y corregir hasta 16 errores dentro de los 223 bytes de datos del bloque [60]. Al ser un estándar ampliamente utilizado, existen implementaciones eficientes de Reed-Solomon con estos parámetros específicos, tanto en software como en hardware. Algunas desventajas de este algoritmo son:

1. Elevado retraso de decodificación: Reed-Solomon es un algoritmo de complejidad temporal asimétrica. Esto significa que el retraso de codificación es mínimo (menos de 10 ciclos de reloj), pero el retraso de decodificación es elevado, pudiendo sobrepasar fácilmente los 1200 ciclos de reloj.

2. Retraso inducido por buffer: si bien el retraso de decodificación es elevado y requiere un procesamiento no despreciable, el tiempo necesario para acumular un bloque de 256 bytes de datos en memoria para comenzar con la decodificación introduce un retraso importante, especialmente si el sistema se utiliza con bajo ancho de banda, tal como es el caso en la implementación acústica.

Ambas desventajas se solucionan ajustando los parámetros de Reed-Solomon para utilizar un menor tamaño de bloque, o bien utilizando un algoritmo similar con menor tamaño de bloque, tal como BCH [61]. Sin embargo, una biblioteca eficiente y disponible que permita el uso de BCH no pudo ser encontrada, por lo que la selección final fue el estándar Reed-Solomon (255, 223).

Para la simulación numérica por software se utilizó la biblioteca *LibFEC* de Phil Karn [62]. Para la implementación en FPGA se utilizó la versión del algoritmo provista de manera gratuita en la biblioteca de núcleos de IP de Xilinx [63].

La implementación del algoritmo Reed-Solomon utilizada posee 32 bytes de paridad y 223 bytes de datos, lo que representa una adición de 14 % a la cantidad total de datos a transmitir. Este código permite corregir hasta 16 errores dentro del bloque, que pueden estar consecutivos, por lo que Reed-Solomon suele utilizarse en canales con errores de tipo *"erasure"* o errores de ráfaga, donde los errores no están uniformemente distribuidos, sino que están agrupados temporal o espacialmente.

### 3.1.2 Características de implementación

Un parámetro importante en la selección del algoritmo es la facilidad de implementación sobre hardware digital. Ciertas características se vuelven importantes al pasar de implementaciones de software a hardware, tales como tamaño, memoria utilizada y velocidad máxima alcanzada con el hardware disponible, con el objetivo de que el sistema funcione a tasas de transferencia en el orden de gigabits por segundo.

A continuación, se listan las características de la implementación en hardware (FPGA) de Reed-Solomon:

El bloque de IP se denomina Reed-Solomon Encoder/Decoder 7.1 de LogiCORE IP. Con respecto al retraso, Reed-Solomon es un algoritmo de complejidad asimétrica, es decir, la complejidad espacio-temporal y ciclomática [64] de los algoritmos de

codificación de Reed-Solomon son diferentes a las de su correspondiente algoritmo de decodificación. En general, la decodificación es más costosa en términos de recursos de hardware y de latencia agregada al sistema. Según la especificación de esta implementación [1], el decodificador Reed-Solomon con configuración CCSDS [65] (que implementa el estándar (255,223)) posee un tamaño de 1364 LUTS (*Look-up tables*, los elementos lógicos de la FPGA) y 3 bloques de RAM. Como comparación, el diseño completo presentado en esta tesis, posee un tamaño de aproximadamente 20000 LUTS, mientras que la FPGA utilizada posee una capacidad de 50000 LUTS. La velocidad máxima de reloj de este algoritmo en la FPGA utilizada es de aproximadamente 350 Mhz, superior a la velocidad requerida por el sistema completo a máxima velocidad, que es de aproximadamente 70 Mhz. La cantidad de recursos utilizados por el codificador es menor: son necesarios sólo 300 LUTS y un bloque de memoria, aunque la velocidad máxima es similar [63].

### 3.1.3 Cálculo de latencia de la etapa de corrección de errores

La latencia en un sistema se define como el tiempo que demora un bit en atravesarlo en su totalidad. Específicamente, el retraso en la etapa de corrección de errores representa un porcentaje importante de la latencia total en la pila de comunicación del sistema. La latencia de un algoritmo es específica a una implementación en particular.

La latencia total estará dada por el retraso introducido por la codificación sumado al retraso introducido por la decodificación, ya que los datos deben atravesar ambas etapas. Sin embargo, el tiempo de latencia en la etapa de codificación es despreciable (del orden de 5 ciclos de reloj [63]), por lo que se utilizarán sólo los valores de latencia de la etapa de decodificación.

La latencia de la etapa de decodificación puede ser calculada de manera exacta mediante ecuaciones provistas por la hoja de datos [1]. Se puede utilizar la figura 3.3 para obtener rápidamente el retraso de procesamiento. El parámetro $t$ se calcula como $t = (n-k)/2$ donde $n$ es la cantidad de símbolos totales en el bloque (en nuestro caso 255) y $k$ es la cantidad de símbolos de datos en el bloque (223 en nuestro caso) por lo que $t = 16$. El retraso total introducido por la decodificación estará dado por la latencia (en nuestro caso es aproximadamente 650 ciclos de reloj) sumado al retraso

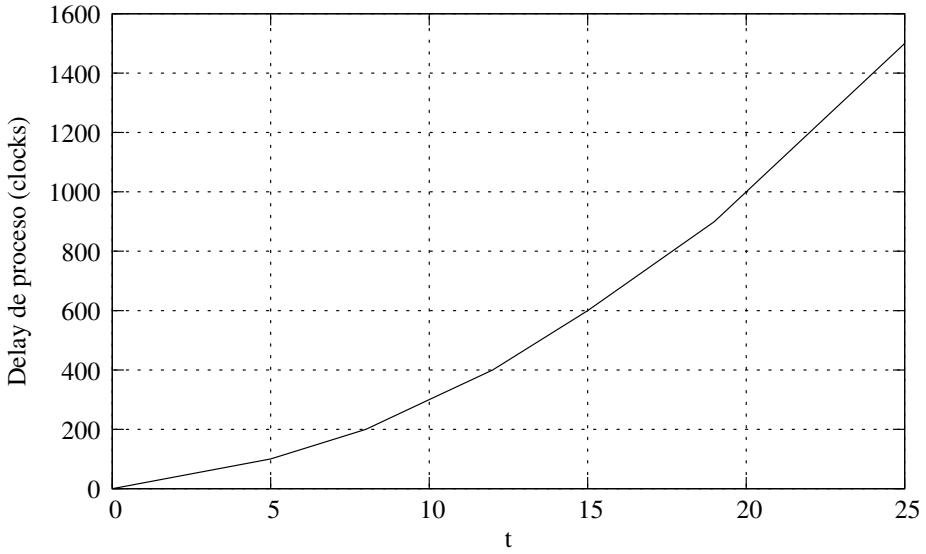



Figura 3.3: Retraso de proceso de la implementación de Reed-Solomon utilizada [1].

producto de cargar un bloque entero de datos en el decodificador. Como los datos deben ingresarse a la memoria del decodificador por medio de un bus serial de un byte de capacidad, se necesitan 255 ciclos adicionales por cada bloque.

Sumando ambos valores, e ignorando la mínima latencia de codificación, podemos afirmar que la latencia introducida por el algoritmo Reed-Solomon en el sistema es de 900 ciclos.

## 3.2 Canal Z con filtros de Bloom

En esta sección se describe el modelo del canal por el cual estamos transmitiendo datos, específicamente el modelo de ruido del mismo. Un canal de comunicaciones puede clasificarse primeramente según el tipo de información transmitida, sea binaria o analógica [66]. Una subclasificación del canal de comunicaciones puede realizarse según el comportamiento del ruido del mismo.

Las comunicaciones digitales suelen modelarse como un canal discreto sin memoria (*discrete memoryless channel*), ya que poseen un alfabeto de símbolos de entrada $A_x$, que son los datos que se desea transmitir, y un alfabeto de símbolos de salida $A_y$ , que son los símbolos detectados por el receptor. El canal es discreto, ya que la cantidad de símbolos posible es finita. Se dice que el canal no posee memoria debido a que la

probabilidad de obtener un símbolo de salida dado no depende de todos los símbolos de entrada, sino solamente del último símbolo enviado.

Otro parámetro importante que define a un canal discreto es la distribución de probabilidades condicionales $P(y|x)$ entre ambos alfabetos, es decir, la posibilidad de que al recibir el símbolo $x$ se haya transmitido el símbolo $y$. Esta distribución puede representarse como un diagrama de distribución de probabilidades (ver figura 3.4) o una matriz.

De acuerdo con la distribución de probabilidades de error que mejor represente al canal físico de transmisión, el tipo de canal que mejor modela las transmisiones digitales por fibra óptica es el denominado canal Z (*Z Channel*), un canal digital en el que el ruido afecta sólo uno de los símbolos binarios a transmitir.

Es este modelo de ruido nos permite innovar en el diseño de algoritmos, adaptándolos y optimizándolos para aprovechar la distribución de ruido, ya que la mayoría de los algoritmos de corrección de errores están pensados para un canal de ruido simétrico y generalmente analógico. Empezaremos primeramente estudiando un modelo simplificado del canal por el cual vamos a trasmitir, el mencionado canal simétrico binario.

## 3.3 Probabilidad de error del canal transmitiendo en un solo slot del frame

Procederemos a calcular la probabilidad de no-colisión de un cliente.

Sea $M$ la cantidad de casilleros por trama y $n$ la cantidad de clientes o usuarios.

Entonces, la probabilidad de no colisión para un usuario en un slot dado es

$$P_{nc} = \left(\frac{M-1}{M}\right)^{n-1} \tag{3.1}$$

Esta ecuación es válida bajo la hipótesis de que todos los clientes eligen el slot a transmitir de manera aleatoria, y de manera independiente. También consideramos que los usuarios utilizan sólo un slot.

Para simplificar, hablaremos de 'colisión' de símbolos cuando uno o más usuarios escriben en el mismo slot de un usuario y causan un error en el canal. De esta manera, en el canal Z, cuando se transmite un 1, las colisiones con símbolos transmitidos por

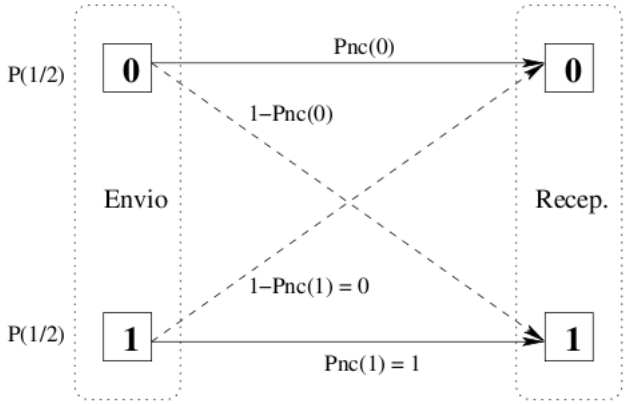



Figura 3.4: Canal binario: esquema de probabilidad.

otros usuarios no causan un error. Diremos, por tanto, que la probabilidad de no colisión de un 1 transmitido es 1, es decir, $P_{nc}(1) = 1$. Por otro lado, cuando se transmite un 0, sólo las colisiones con 1s transmitidos por otros usuarios generan error en el canal.

Siendo $P_{nc}(1)$ la probabilidad de no colisión del símbolo uno, y $P_{nc}(0)$ la probabilidad de no colisión del símbolo cero, la probabilidad total de no colisión para un usuario en un canal Z es

$$P_{nc} = P(1) \cdot P_{nc}(1) + P(0) \cdot P_{nc}(0) \tag{3.2}$$

Asumiendo que todos los usuarios transmiten un stream de datos aleatorio, tenemos que $P(1) = P(0) = \frac{1}{2}$. Entonces podemos desarrollar $P_{nc}$ como

$$P_{nc} \;=\; \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \sum_{i=0}^{n-1} C_i^{n-1} \left(\frac{M-1}{M}\right)^i \left(\frac{1}{M}\right)^{n-1-i} \left(\frac{1}{2}\right)^{n-1-i} \tag{3.3}$$

La complejidad de la ecuación 3.2 se encuentra entonces en el desarrollo de $P_{nc}(0)$. Cada término de la sumatoria del segundo término del RHS de la ecuación 3.3 da la probabilidad de que $(n - i - 1)$ usuarios escriban un 1 en el slot seleccionado. El factor $C_i^{n-1}$ suma sobre todas las combinaciones posibles de canales que no hayan colisionado, que son hechos independientes. Luego, $\left(\frac{M-1}{M}\right)^i$ es la probabilidad de no

colisión de $i$ canales (se suma para todo posible número de canales no colisionando: $1 \leq i \leq n$, que están en otro casillero), $\left(\frac{1}{M}\right)^{n-1-i}$ es la probabilidad de colisión de los restantes $n-1-i$, y la colisión se produce cuando los otros canales transmiten el símbolo 1 cuya probabilidad es $\left(\frac{1}{2}\right)^{n-1-i}$.
Teniendo en cuenta que $\sum_{i=0}^{n-1} C_i^{n-1} \left(\frac{M-1}{M}\right)^i \left(\frac{1}{2M}\right)^{n-1-i}$ es la potencia $n-1$ de un binomio, tenemos

$$P_{nc} = \frac{1}{2} + \frac{1}{2} \cdot \left(\frac{M-1}{M} + \frac{1}{2M}\right)^{n-1} \tag{3.4}$$

$$P_{nc} = \frac{1}{2} + \frac{1}{2} \cdot \left(1 - \frac{1}{2M}\right)^{n-1} \tag{3.5}$$

$$P_{nc} \simeq \frac{1}{2} + \frac{1}{2} \cdot e^{\frac{-n}{2M}} \tag{3.6}$$

Es decir, la probabilidad de no colisión depende de la relación $n/M$. Si $M >> n$, entonces $P_{nc}$ se aproxima a 1, que es una característica deseable en el sistema.

### 3.3.1 Capacidad de canal

Existe una relación entre la probabilidad de error $Pb$ de un canal y la máxima velocidad de transmisión de datos posible en el mismo. Esta relación fue estudiada por Claude Shannon en 1948 en un artículo pionero de la teoría de la información [14] y es conocida actualmente como teorema de Shannon-Hartley, también llamado teorema de codificación de canales con ruido (*noisy channel coding theorem*).

La capacidad $C$ de un canal discreto sin memoria es la máxima información mutua entre los alfabetos $X$ de entrada e $Y$ de salida:

$$C = \max_{\mathcal{P}_x} I(X;Y) \tag{3.7}$$

Para hallar el máximo podemos derivar $I(X;Y)$ con respecto a la probabilidad $P_x$. De [66], para un canal binario simétrico sin memoria con probabilidad de error $p$, la capacidad máxima $C$ es:

$$C \approx 1 - H(p) \tag{3.8}$$

donde $H(p)$ es la función de entropía binaria

$$H(p) = [p \cdot log_2(p) + (1-p) \cdot log_2(1-p)] \tag{3.9}$$

Si expandimos $H(p)$ en 3.8:

$$c = 1 - \left( p \cdot \log_2 \left( \frac{1}{p} \right) + (1-p) \cdot \log_2 \left( \frac{1}{1-p} \right) \right)$$

Simplificada:

$$c = 1 + p \cdot \log_2(p) + (1-p) \cdot \log_2(1-p)$$

En la figura 3.6 puede verse la evolución de la capacidad del canal binario simétrico, que es máxima para $p = 0$ y $p = 1{,}0$, mientras que es cero para $p = 0{,}5$, ya que con 0 % de probabilidad de error la capacidad es la máxima (no hay interferencia) y con 50 % de error la capacidad es cero y es imposible transmitir dato alguno. Quizás contra intuitivamente, con 100 % de posibilidad de error, la capacidad también es máxima, ya que equivale a invertir cada símbolo transmitido, operación que no introduce error alguno en los datos.

### 3.3.2 Canal Z

Un canal Z difiere de un canal binario, ya que las probabilidades de error de bit son asimétricas. Los canales Z se usan generalmente para modelar sistemas de transmisión ópticos.

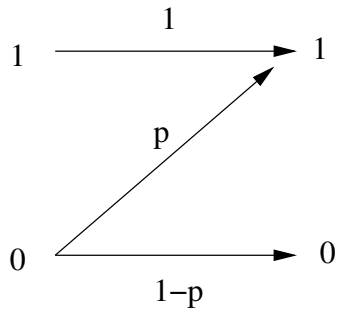



Figura 3.5: Diagrama: canal Z. El diagrama superior podría representar un canal de fibra óptica donde un 1 representa el Láser encendido.

Para un canal Z, la distribución de probabilidades de la información mutua $I(X;Y)$ es diferente a la de un canal binario simétrico [67], por lo que obtenemos un máximo diferente:

$$C_Z = 1 - \left(\frac{1}{2} * H(p)\right) \tag{3.10}$$

Por lo tanto, expandiendo $H(p)$ (definida en 3.9) en 3.10:

$$C_Z = \log_2 \left(1 + (1-p)p^{p/(1-p)}\right)$$

La diferencia entre las capacidades de ambos tipos de canal puede apreciarse en la figura 3.6. El mínimo de capacidad en el canal simétrico se da cuando $p = 0{,}5$, mientras que en el canal asimétrico, el mínimo de capacidad se produce cuando $p = 1{,}0$.

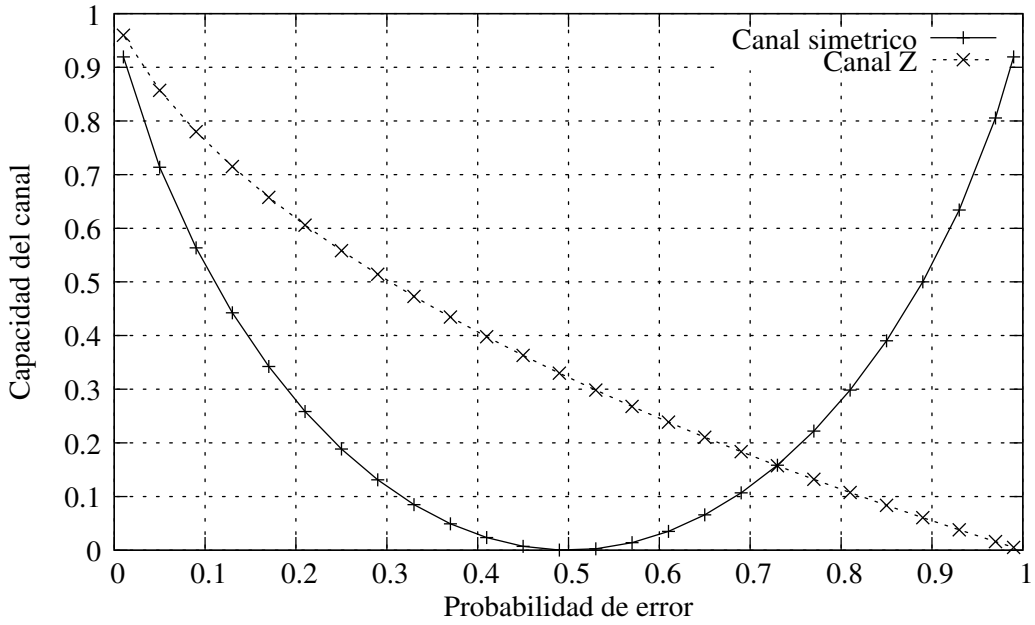



Figura 3.6: Capacidad de un canal binario simétrico con respecto a uno asimétrico o canal Z.

## 3.4 Filtros de Bloom

Como se discutió en la sección 2.4 , la colisiones de símbolos son inherentes al tipo de codificación seleccionada. En la modulación OOK (*on-off keying*) utilizada en un medio óptico, sólo los '1's transmitidos pueden interferir con '0's. Este comportamiento puede ser modelado como un canal-Z porque la superposición de pulsos de luz individuales representando '1's puede solamente ser identificados como un '1's. De esto se desprende que un '0' recibido es un signo inequívoco de la ausencia de pulsos en el casillero de tiempo leído. Una buena estructura para representar este tipo de datos es el filtro de Bloom [68], que se utiliza comúnmente como función de *hash* [69]. Dichas funciones constituyen una familia de algoritmos utilizados como tests eficientes (complejidad temporal $O(1)$) de pertenencia de un miembro en un conjunto, a diferencia de una búsqueda normal que puede tener una complejidad temporal mucho mayor (podemos citar el algoritmo de búsqueda binario, con una complejidad de $O(log_2(n))$.

La manera en que se implementó este algoritmo en el sistema propuesto se basa en copiar cada bit en $K$ casilleros de la trama transmitido, siendo la trama la representación física del filtro de Bloom. En el extremo receptor es suficiente recibir un solo '0' entre las $K$ copias del bit, para inferir que el bit original era originalmente un '0', mientras que si el bit original era un '1', las colisiones no tienen efecto debido a la naturaleza del canal-Z.

En la figura 3.7 puede apreciarse gráficamente como se utiliza un filtro de Bloom para la transmisión de 12 clientes con una repetición $K = 3$.

### 3.4.1 Filtros de Bloom encriptados

En esta etapa se realiza la encriptación de los datos, reemplazando el algoritmo de hashing que selecciona las posiciones de los datos dentro del filtro de Bloom por una función pseudoaleatoria criptográficamente segura, de modo que los bits de datos de los diferentes clientes se posicionan aleatoriamente en la trama, y sólo es posible decodificar los datos si se tiene exactamente la misma secuencia pseudoaleatoria con que fueron posicionados originalmente. Como esta secuencia está determinada por la semilla del algoritmo PRNG, los participantes deberán compartir esta semilla

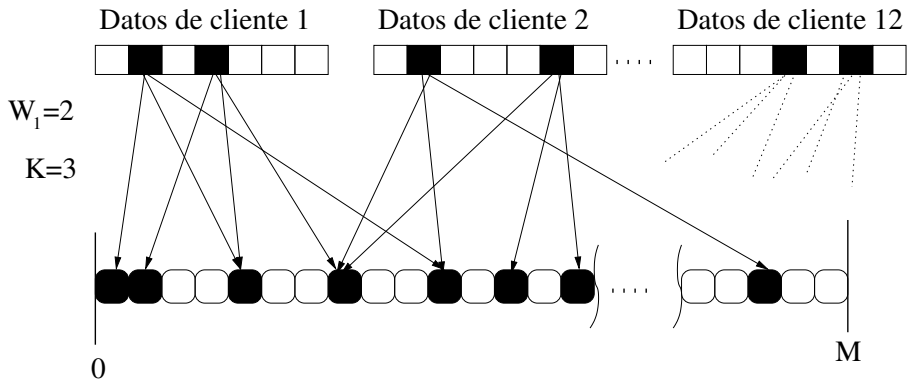



Figura 3.7: Filtro de Bloom. M es el largo de la trama. $W_1$ es el peso de Hamming mínimo. El parámetro K es el número de repeticiones.

previamente, que es el equivalente a una clave o *password* simétrico.

Desde el punto de vista de la modulación, el algoritmo PRNG selecciona la posición temporal dentro de la trama, por lo que este esquema es equivalente a una transmisión time hopping, con la única salvedad de que el algoritmo de filtro de Bloom requiere $K$ repeticiones de los datos para poder recuperarlos de colisiones en la recepción.

Para poder decodificar los datos en el filtro de Bloom receptor es necesario que todos los participantes posean la misma secuencia pseudoaleatoria, es decir, la misma clave o semilla generadora 2.3 del mismo PRNG utilizado para codificar los datos, y todos deben estar sincronizados a nivel de trama con el nodo originante. Las tramas del cliente originante y el receptor deben empezar y terminar al mismo tiempo para poder regenerar exactamente todas las posiciones en donde se transmitieron los datos.

Sin embargo, los demás clientes que utilizan el medio compartido sólo causan interferencia y por lo tanto la sincronización a nivel de trama sólo es necesaria entre los clientes que deseen compartir el canal encriptado. Esto reduce los requerimientos de sincronización y simplifica la implementación de la red.

Finalmente, es deseable, pero no necesario, que todos los clientes mantengan una sincronización a nivel de bit, es decir, que los tiempos de transmisión de todos los clientes estén suficientemente alineados para que el casillero de un cliente sólo pueda superponerse con otro casillero de otro cliente y le cause un solo error de bit. Si esta sincronización no se mantiene, un casillero podría interferir con dos casilleros de otro cliente que está desalineado con respecto al primero, provocando dos errores en lugar

de uno solo y aumentando los requerimientos de corrección de errores en el sistema.

## 3.5 Minimización de peso de Hamming

El esquema propuesto, basado en time-hopping CDMA, utiliza la interferencia entre símbolos para obtener confidencialidad, ya que los datos de los otros usuarios actúan efectivamente como ruido. La interferencia intersímbolo, como fue discutida en la sección 2.1, causa errores en la comunicación que deben ser corregidos. Para reducir la interferencia, no es aconsejable modificar o introducir patrones en el generador criptográficamente seguro de números aleatorios, ya que comprometería la seguridad de todo el sistema al existir la posibilidad de introducir factores que permitan predecir las posiciones de los símbolos (ej. usando códigos ortogonales como en Ref. [70].), efectivamente dejando de ser criptográficamente seguro.

Considerando que el medio de transmisión se adecua a un canal Z, se propone aprovechar la naturaleza asimétrica de este tipo de medio, en donde solamente el símbolo "1" causa interferencia. [2] En otras palabras, la interferencia de un canal Z es proporcional al peso de Hamming ($HW$) del símbolo transmitido. En esta sección se presenta un algoritmo que minimiza este valor, con el objetivo de causar menor interferencia. El algoritmo de minimización de peso de Hamming consiste en una codificación en donde cada símbolo binario es convertido en un equivalente de mayor longitud, que posee una mínima cantidad de dígitos en "1". Aplicando esta codificación y transmitiendo el símbolo resultante, se obtiene una menor interferencia, siempre y cuando el medio de transmisión pueda modelarse como un canal Z. Intuitivamente, expandir el símbolo original a uno de mayor longitud reduciría el ancho de banda del canal; pero como las simulaciones numéricas muestran (ver sección 4) a medida que la interferencia intersímbolo disminuye, el ancho de banda adicional utilizado por los algoritmos de FEC también se reduce, compensando por el incremento del largo del símbolo, y logrando un mayor ancho de banda efectivo del sistema. Podemos decir que un número binario normal de largo $L$ posee un $HW$ variable, con $L/2$ siendo el

[2] Aunque en un sistema de comunicaciones ópticas real, existe una pequeña diferencia ya que el nivel de "0" no es representado con una potencia de cero Watts.

| Datos | entrada HW= 0 a 3 | Expandida HW=2 |
|---|---|---|
| 0 | 000 | 00011 |
| 1 | 001 | 00110 |
| 2 | 010 | 00101 |
| 3 | 011 | 01100 |
| 4 | 100 | 01010 |
| 5 | 101 | 01001 |
| 6 | 110 | 10001 |
| 7 | 111 | 10010 |

Cuadro 3.1: Tabla de minimización de Hamming para símbolos de 3 bits. Esta tabla puede utilizarse para convertir datos de entrada (números del 0 al 7 y su representación binaria) en su representación con peso de Hamming minimizado, en la tercer columna. El peso de Hamming de los símbolos de entrada es variable de 0 a 3, y el de salida es siempre 2.

promedio, cero siendo el mínimo y $L$ siendo el $HW$ máximo. La técnica de reducción logra que $HW = 2$, siendo este valor un balance apropiado entre la reducción de interferencia y el largo de símbolo. Adicionalmente, es deseable en un sistema de seguridad que no se revele ninguna información acerca de los símbolos transmitidos. Por ejemplo, si transmitiéramos el número cero, representado por todos sus dígitos en cero, sería trivial identificarlo debido a la ausencia de dígitos en uno, condición fácilmente detectable. Para evitar este tipo de actividad maliciosa o "ataques" que utilizan análisis estadísticos de los datos, la codificación exige que el peso de Hamming sea fijo en todos los símbolos. Esto causa una ligera pérdida en el ancho de banda, pero hace imposible inferir cualquier tipo de información acerca de los datos transmitidos analizando estadísticas de tráfico.

## 3.6 Expansión de símbolo

La minimización del peso de Hamming conlleva una necesaria conversión del símbolo original a otro que tendrá mayor longitud, es decir, una expansión del símbolo. Esta operación puede realizarse de muchas maneras, pero un algoritmo eficiente es la tabla de lookup (ver tabla 3.1), donde un símbolo de largo L es utilizado como el índice en una tabla, y la salida se encuentra en la segunda columna de la misma tabla,

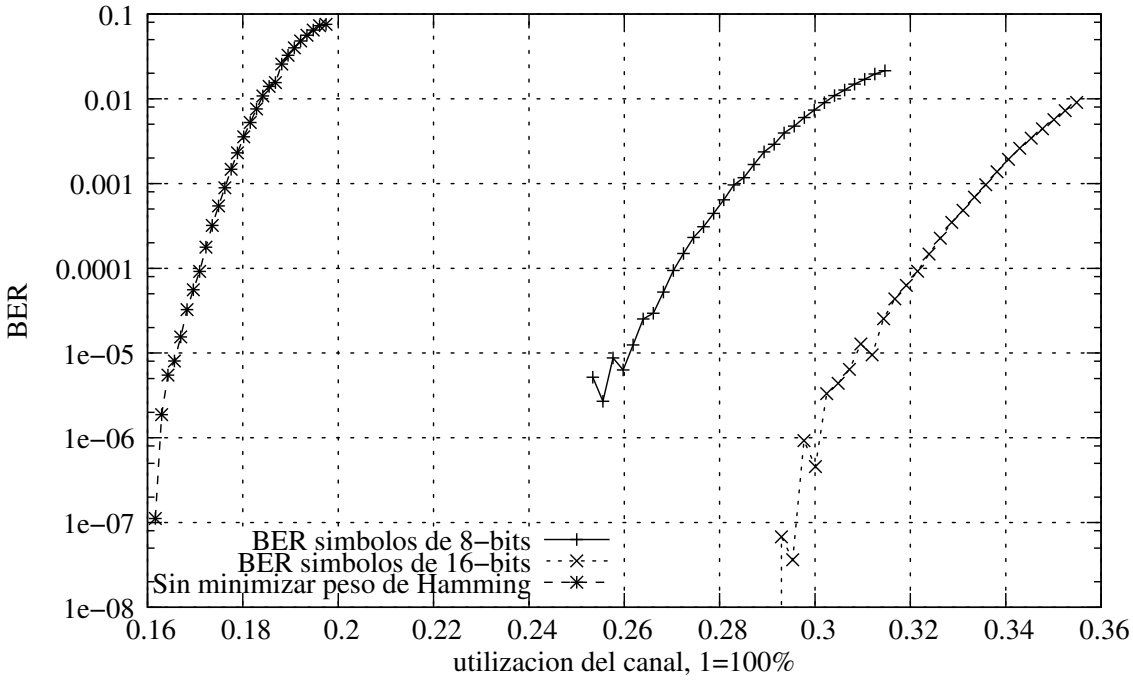



Figura 3.8: Desempeño del sistema con respecto a la expansión de símbolo. Simulación numérica de un enlace de 10 Gbps con 128 clientes, M=4096 y K=9.

donde estará almacenado el símbolo expandido de largo N, siendo que $N>L$. Por motivos prácticos y de optimización, es deseable que $L$ sea múltiplo de 8. Al aplicar la minimización de $HW$ a símbolos de 8 o 16 bits de longitud, son necesarios 256 o 65536 símbolos de salida, respectivamente, cada uno con un $HW = 2$. En el caso de símbolos de entrada de 8 bits, la longitud del símbolo de salida será de 363 bits, mientras que, para 8 bits de entrada, el símbolo expandido con $HW = 2$ tendrá 24 bits de longitud. Puede observarse que el número de símbolos únicos con $HW = 2$ y $N = 363$ no es exactamente 65536 sino 65703. Esto significa que la tabla de expansión no es única, sino que existen muchas tablas funcionalmente equivalentes que pueden seleccionarse. Cada tabla posible producirá un conjunto único de símbolos con $HW = 2$, por lo que a pesar de ser equivalentes, los nodos participantes deberán necesariamente utilizar idénticas tablas para la codificación y decodificación.

La Figura 3.8 muestra tres simulaciones: una sin expansión, otra con una expansión de 8 bits y otra de 16 bits. En dicha figura se muestra el BER en función de la utilización del canal (el porcentaje real de uso por la totalidad de los clientes cuando

se elimina todos los bits extras de las codificaciones, es decir, la capacidad que la suma de usuarios vería sin este sistema). Como se puede apreciar, hay una mejora substancial en el aprovechamiento del canal: para un BER de $10^{-6}$ tenemos 0.16, 0.25 y 0.3 aproximadamente. Es decir que con 8 bit mejoramos un 50 % del original, y con 16 bis un 87 %.

## 3.7 Probabilidad de colisión de filtro de Bloom con expansión de símbolo

En esta sección, presentaremos una estimación analítica de la probabilidad de error de bit, tomando en cuenta sólo las interferencias de otros usuarios en la red. No consideraremos ninguna corrección de etapas o algoritmos adicionales como Reed-Solomon, o interferencias producidas en el medio físico. Como se explicó en la sección 3.4, cada usuario agrupa sus bits de información en paquetes o tramas de largo $n$. Cada paquete es codificado utilizando exactamente $m_1$ unos y $m_0$ ceros, siendo $m$ la cantidad de bits de la trama, donde

$$m = m_1 + m_0$$

.

Debido a la utilización del filtro de Bloom, cada uno de los $m$ dígitos binarios resultantes es repetido $K$ veces en posiciones elegidas aleatoriamente en la trama de largo $M$. Las K repeticiones de un dígito binario pueden colisionar con otras repeticiones del mismo dígito, con repeticiones de otro dígito o bien con dígitos pertenecientes a otro cliente. Llamaremos $N$ al número de usuarios activos. Para estimar la tasa de error o BER (Bit Error Rate) del sistema y simplificar los cálculos, asumiremos lo siguiente:

1. Las tramas de diferentes usuarios están sincronizadas, es decir, cada usuario participante del canal de comunicaciones recibe la misma trama en el mismo orden, y cada trama contiene (incluyendo colisiones) $W_0 = N \cdot K \cdot m_0$ ceros y $W_1 = N \cdot K \cdot m_1$ unos.

2. No incluiremos en el análisis la posibilidad de corrección de errores debido a que, en general,

$$\left( \begin{array}{c} m \\ m_1 \end{array} \right) > 2^n. \tag{3.11}$$

Específicamente, cada vez que una secuencia errónea de $m$ dígitos binarios es recibida con más de $m_1$ unos, se decodifica como una cadena de bits aleatoria de largo $n$. Por lo tanto, el número esperado de errores será $n/2$.

Definiremos las siguientes probabilidades: $P_{s1}$ como la probabilidad de sobre-escribir con unos las $K$ repeticiones de por lo menos uno de los $m_0$ ceros. $P_{st}$ como la probabilidad de sobrescribir con unos todas las $K$ repeticiones de uno de los $m_0$ ceros.

Entonces, el BER está dado por

$$\text{BER} = \frac{n}{2} P_{s1}. \tag{3.12}$$

Por la cota de la unión (union bound),

$$P_{s1} m_0 \leq P_{st}. \tag{3.13}$$

Por lo tanto, prestemos atención a uno de los $m_0$ ceros. Si los $W_1$ transmitidos (por todos los usuarios) ocupan $s$ casilleros y las $K$ repeticiones del cero dado usa $r(\leq K)$ casilleros, entonces una condición necesaria para el error es que $s \geq r$. Entonces, para que haya un error necesitamos que existan $s$ unos en una trama de $M$ bits. Dados $r$ lugares en la trama, la probabilidad de que los unos ocupen esas $r$ posiciones está dada por

$$z_{r,s} = \frac{\left( \begin{array}{c} M-r \\ s-r \end{array} \right)}{\left( \begin{array}{c} M \\ s \end{array} \right)} = \frac{\frac{(M-r)!}{(M-s)!(s-r)!}}{\frac{M!}{(M-s)!s!}} = \frac{(M-r)!}{M!} \frac{s!}{(s-r)!} \approx (\frac{s}{M})^r, \tag{3.14}$$

donde en la aproximación hemos supuesto que $N, s \gg r$. Si $M \gg K$, no es difícil ver que las $K$ repeticiones de un cero dado ocupan $\mu_R \approx K$ casilleros en promedio.

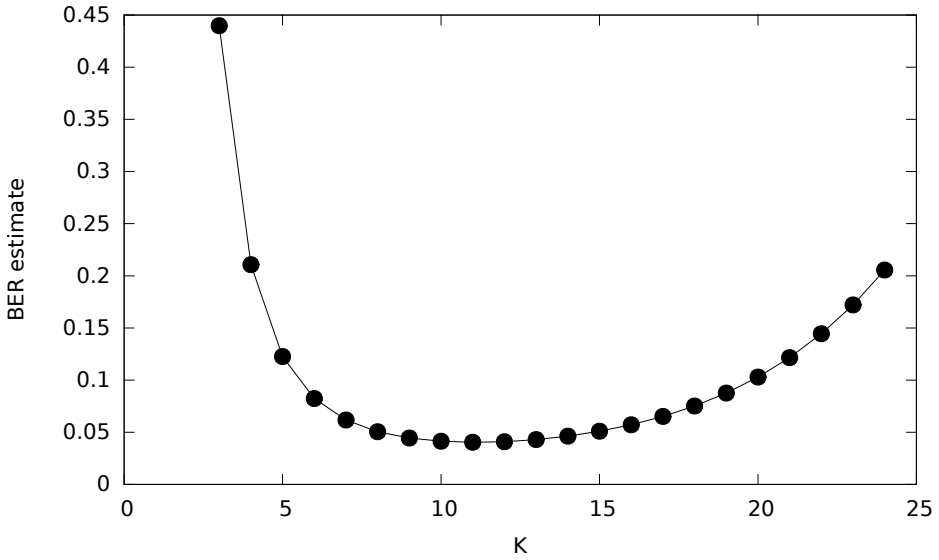



Figura 3.9: Estimación de BER vs. tasa de repetición de filtro de Bloom K.

También puede demostrarse que el número promedio de casilleros ocupados por los $W_1$ unos transmitidos por todos los usuarios es

$$\mu_S \approx M(1 - e^{-W_1/M}) \tag{3.15}$$

De esas ecuaciones, una estimación de la cota superior del BER para un determinado usuario es

$$\text{BER} \lessapprox \frac{n}{2} m_0 z_{\bar{R},\bar{S}} \approx \frac{n}{2} m_0 \left(1 - e^{-W_1/M}\right)^K . \tag{3.16}$$

La figura 3.9 muestra la estimación en función de $K$ para $M = 2014$, $m_0 = 22$, $m_1 = 2$, $n = 8$ y $N = 38$. Es interesante notar que existe un valor óptimo de la tasa de repetición $K$ que minimiza la tasa de error. Este resultado es relevante en el diseño de un sistema de comunicaciones. Debido a los bajos valores de BER alcanzados, es posible utilizar en la siguiente etapa algoritmos eficientes que aceptan bajos límites de error, tal como Reed-Solomon, para reducir aún mas el BER total de sistema y así llevarlo a tasas aceptables para aplicaciones prácticas.

## 3.8 Códigos de pseudoruido

Como se explica en la sección 2.3 la seguridad del sistema depende de la correcta selección e implementación de un algoritmo de PRNG criptográficamente seguro *(CS-PRNG)*. El sistema impone una restricción adicional a esta etapa, ya que además de cumplir con todas las propiedades de un CS-PRNG, se debe seleccionar un algoritmo eficiente ya que se necesitará generar una posición aleatoria por cada bit que se desea transmitir. Por lo tanto, es deseable maximizar la cantidad de bits por ciclo de reloj que el CS-PRNG es capaz de generar. En el caso de la implementación para el transceptor óptico sobre una FPGA, el algoritmo seleccionado para el prototipo inicial fue el denominado ARC4, debido a la simplicidad, bajo consumo de recursos de hardware y alta velocidad del mismo [9]. Si bien existen implementaciones de alta performance [71], estas no son fácilmente accesibles ni disponibles, por lo que se reimplementó este algoritmo íntegramente, utilizando el lenguaje de descripción de hardware Verilog [72], utilizando optimizaciones para lograr la performance deseada de 1 byte pseudoaleatorio generado por cada ciclo de reloj. Es necesario tener en cuenta es que ARC4 es un algoritmo relativamente anticuado y recientemente varios ataques estadísticos han puesto en duda su utilización como generador criptográficamente seguro [73], por lo que en implementaciones futuras es recomendable que sea reemplazado por un algoritmo criptográfico moderno.

En las implementaciones de software o acústicas, el poder de procesamiento necesario para esta etapa se reduce, ya que la velocidad de reloj de un CPU suele ser elevada con respecto a la velocidad posible en este medio de transmisión, por lo que no es necesario que el algoritmo PRNG tenga un rendimiento elevado.

### 3.8.1 Aplicación al algoritmo de filtro de Bloom encriptado

Este algoritmo asigna los tiempos de transmisión de $r$ clientes, seleccionándolos entre $M$ posiciones, correspondientes a los $M$ casilleros dentro de la trama de transmisión. La cantidad posible de combinaciones de $M$ posiciones entre todos los clientes es de ${}_{M}P_{r} = \frac{M!}{(n-r)!}$. Consideraremos que un ataque a este algoritmo fue exitoso cuando un atacante puede inferir la serie de posiciones $M$ para un cliente, obteniendo así todos

sus datos.

Existe un algoritmo de selección de $M$ que suponemos no posee ninguna debilidad, es decir, selecciona $r$ conjuntos de $M$ posiciones tal que, aún si el atacante pudo adquirir un número arbitrario de las posiciones de transmisión pasadas, no puede predecir ninguna de las posiciones futuras.

Esto puede cumplirse simplemente asignando a cada canal de transmisión seguro su propio algoritmo generador pseudoaleatorio criptográficamente seguro, o bien el mismo algoritmo utilizando claves diferentes. Esto provocará colisiones entre los clientes, es decir, al asignarse posiciones de transmisión de manera aleatoria, existirán coincidencias donde a dos o más clientes se les asignará el mismo casillero dentro de la trama. Esto es resuelto mediante corrección de errores en capas superiores y para el cálculo del parámetro de seguridad se despreciará este efecto.

Dadas las siguientes suposiciones:

- El algoritmo de selección pseudoaleatorio no tiene debilidades.
- El atacante no posee control de los datos a transmitir, y estos son totalmente aleatorios.

Un atacante podría tratar de predecir el conjunto de posiciones $n$ de un cliente, para obtener sus datos. Para ello, deberá probar exhaustivamente todo el conjunto de ${}_M P_r$ sobre una trama capturada, o bien probar todas las combinaciones posibles de la clave del generador pseudoaleatorio. De esto se desprende que si $largo(clave) > 128\ bits$ y $M > 128$ se considera que el algoritmo cuenta con un nivel de seguridad denominada "fuerte", ya que una complejidad temporal de $2^{128}$ es considerada segura al momento de la escritura de esta Tesis [74].

### 3.8.2 Problemas de símbolos con peso de Hamming variable

En la sección anterior se nombraron dos condiciones necesarias. La primera condición, la carencia de vulnerabilidades en el algoritmo CS-PRNG, es necesaria e inevitable por motivos obvios. Sin embargo, es posible eliminar la segunda condición, de precisar datos totalmente aleatorios, realizando una modificación a la tabla de expansión. Esto

es posible ya que la segunda condición es sólo necesaria para prevenir el siguiente escenario donde la seguridad falla:

Supongamos que se desea transmitir dos bytes:

- El byte 0 (00000000 en representación binaria)

- Y el byte 255 (11111111 en representación binaria)

La tabla de expansión convierte los símbolos de 8 bits en símbolos de 16 bits, con peso de Hamming $HW <= 2$. Supongamos que la tabla asignó al valor 0, el símbolo 0000000000000000 y al valor 255 el símbolo 0000100010000000. Ambos símbolos de salida cumplen con la condición de $HW <= 2$. Al transmitirse estos bytes, las posiciones son aleatorizadas y transmitidas.

Ignorando momentáneamente las colisiones, un atacante que observa el tráfico puede reconocer qué byte esta siendo transmitido, aún cuando la posición de cada bit este aleatorizada, simplemente contando la cantidad de unos, es decir, el peso de Hamming variable está revelando al atacante información acerca de los datos transmitidos, aún cuando los símbolos fueron permutados.

Éste ataque puede eliminarse generando una tabla de expansión cuyo peso de Hamming de símbolos de salida sea estrictamente un valor fijo. Es decir, para evitar el ataque en el ejemplo anterior, los símbolos de salida en lugar de tener $HW <= 2$ deben cumplir con la condición de $HW = 2$.

De esta manera, al convertir los datos de entrada en símbolos uniformes con el mismo largo y el mismo peso de Hamming [3], los bits de salida del algoritmo serán completamente aleatorios sin importar los datos de entrada y el atacante no podrá inferir ninguna información acerca de la comunicación.

[3]Si el peso de Hamming es $P$, el atacante podrá observar un peso de Hamming de 1 hasta $P$, y no siempre $P$, esto es debido a las colisiones de bit que un símbolo transmitido por un cliente tendrá con sí mismo.

## 3.9 Resumen del sistema completo

El sistema propuesto, cuyo diagrama de alto nivel se muestra en la figura 3.2, está compuesto primeramente de una capa de acceso, donde se encuentra la implementación de la codificación CDMA y la corrección de errores, y una capa física basada, o bien en una red óptica con similitudes a redes PON 2.6.5 , o una red acústica de tipo difusión (*broadcast*). La capa de acceso está implementada utilizando técnicas CDMA del tipo time-hopping, donde cada uno de los clientes posibles codifica su información en bits y los transmite en un casillero seleccionado de manera aleatoria dentro de una trama de $M$ casilleros[4]. De esta manera, ocurrirán múltiples colisiones entre diferentes ONUs *(optical network unit)*, pero los errores causados por estas colisiones serán corregidos por la capa de corrección que garantiza una transmisión de datos confiable. Aunque es imposible eliminar totalmente los errores, consideramos una transmisión con un BER de 10e-12 como libre de errores.

Si bien existe el requerimiento de que todos los clientes comunicantes deben estar sincronizados a nivel de trama para regenerar correctamente las posiciones de transmisión, esta sincronización no es necesaria para clientes que no participen del canal encriptado. Un cliente $X$ puede recibir mensajes de otro cliente $Y$ si y sólo si $X$ posee la *clave* de $Y$, y viceversa. De esta manera, si un cierto grupo de clientes desea comunicarse sobre un canal encriptado, es necesario cada cliente en el grupo conozca la *clave*. El canal encriptado que se forma entre los clientes forma un "dominio de difusión" ya que todos los datos que transmita un cliente serán recibidos sólo por los otros clientes participantes del dominio. Este dominio es análogo al sistema VLAN *(Virtual Local Area Network)* de particiones lógicas de red.

Los datos de los clientes se codifican con las siguientes técnicas de corrección de errores: Reed-Solomon (223/255) (ver [8] y sus referencias), y un filtro de Bloom[68].

En principio, se utilizó un algoritmo LDPC 2.1.2 (Con matriz de $1024 \times 512$) pero fue descartado en posteriores iteraciones del diseño, ya que al agregar la optimización de la expansión de símbolo al filtro de Bloom, se incrementó la capacidad de corrección del mismo y pudo eliminarse la etapa de corrección de errores de tipo LDPC, con el

[4] El parámetro $M$ debe optimizarse en función del nivel de error aceptable y la máxima cantidad de clientes soportados.

consiguiente aumento de la capacidad total del sistema.

En la selección de los algoritmos de corrección de errores siempre se utilizó el canal Z como modelo del canal de comunicaciones.

## 3.10 Aplicación en distintos medios físicos

Al poseer una fuerte capacidad de corrección de errores, la arquitectura del sistema lo hace confiable frente a todo tipo de interferencias de la capa física, por lo que modificando la etapa de modulación pueden utilizarse diferentes medios físicos, siempre que los mismos puedan modelarse como un canal Z.

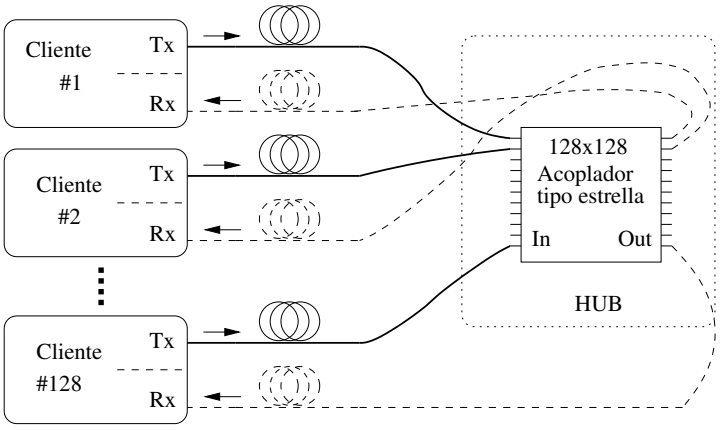
### 3.10.1 Redes ópticas

Al adaptar el sistema propuesto a una red óptica, la topología física debe ser de tipo estrella (ver Fig.3.10) donde splitters ópticos redistribuyen el tráfico proveniente de cada ONU a todo el resto de los terminales, permitiendo comunicaciones punto a punto así como punto a multipunto, con una cantidad máxima de hasta 128 ONUs simultáneas. Este límite esta dado por las atenuaciones causadas por la fibra óptica y por el concentrador que el sistema debe ser capaz de compensar mediante amplificación.

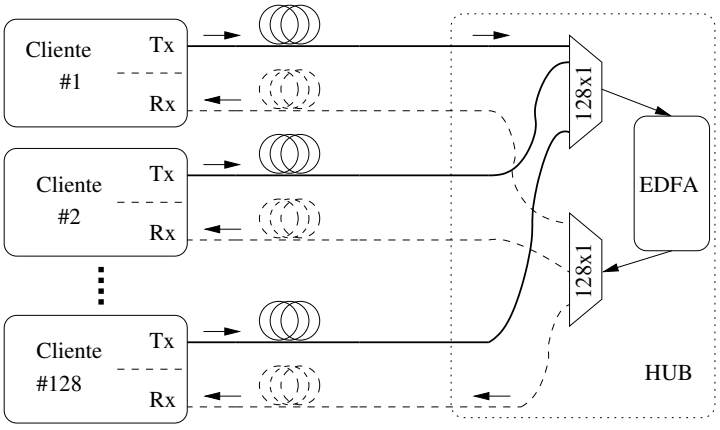
Un amplificador óptico de tipo EDFA *(Erbium-Doped Fiber Amplifier)* localizado entre los splitters incrementa la potencia óptica para compensar las perdidas en la red, aunque esto es solamente necesario en distancias entre clientes superiores a 10 km.

La modulación utilizada para las señales ópticas es RZ o *Return to Zero*, con velocidades previstas de hasta 10 Gbps, utilizando un Láser DBF *(Distributed Feedback)* de 2 dBm de potencia y 1550 nm de color/frecuencia. Estos parámetros permiten una transmisión de hasta 10 km entre los nodos si se utiliza fibra óptica mono modo estándar (ITU-T G.652).

En el concentrador, un splitter de $128 \times 1$ concentra el tráfico de todos los ONUs y es luego redistribuido por el correspondiente splitter de $1 \times 128$, canalizando el tráfico combinado de cada ONU a través de las fibras ópticas. Este splitter permite tener




(a) Distribución via acoplador tipo estrella 1




(b) Distribución via EDFA

Figura 3.10: Diseño de red propuesto para la capa óptica: un acoplador de tipo estrella es la base para la arquitectura de red en distancias inferiores a 10 km. Para extender el alcance de la red, un amplificador óptico del tipo EDFA *(Erbium-Doped Fiber Amplifier)* puede ser utilizado en el concentrador central.

hasta 128 ONUs en el sistema.

La atenuación de los splitters centrales ($\simeq$ 25 dB cada uno) sumada a la atenuación propia de la fibra óptica ($\simeq$ 2 dB por tramo) y pérdidas por inserción (aproximadamente $\simeq$ 1 dB) contribuyen a la elevada atenuación que el amplificador debe compensar ($\simeq$ 28 dB).

De utilizarse sin ningún tipo de amplificación, la atenuación que una señal sufriría entre dos ONUs es la suma de la atenuación de ambos tramos, es decir $\simeq$ 56 dB, que es un valor que supera el límite de la tecnología de detección comercial disponible al momento de la escritura de esta Tesis, teniendo en cuenta potencias de transmisión

máximas de 2 dBm.

Sin embargo, es posible utilizar etapas de amplificación intermedias para obtener niveles de señal adecuados. Para proveer la amplificación requerida, un EDFA con $\geq$ 27 dB de ganancia es colocado entre ambos splitters. Este EDFA incrementa la potencia del tráfico a la salida del primer splitter, elevando la potencia de cada '1' de $\simeq -26$ dBm a 1 dBm a la entrada del segundo splitter, que será atenuada nuevamente a un nivel de potencia de $-27$ dBm, valor dentro de los parámetros aceptables de un fotodetector de alta sensibilidad (aproximadamente $-28$ dBm [75]).

Aún considerando una ganancia de EDFA constante, la potencia óptica a la entrada del detector PD sería menor ($-17$ dBm) que la requerida por dispositivos comerciales ($\sim -5$ dBm). El nivel de bit '0' es dado por la adición de todos los bits '0' transmitidos por las 128 ONUs. Por lo tanto, el nivel de decisión del receptor debería ser capaz de separar entre este estado (la suma de los bits '0') y aquel de un simple ONU transmitiendo un solo bit en '1'. De esto se desprende que la potencia de transmisión del bit '0' debe ser la menor posible, o lo que es lo mismo, la *relación de extinción* del láser DBF debe ser alta.

### 3.10.2 Redes acústicas

Un canal óptico es un claro ejemplo de canal Z, pero también es posible realizar un canal Z con redes acústicas si se utilizan ciertas modulaciones.

Los enlaces ópticos presentan como mayor desventaja la necesidad de, o bien transmitir los pulsos de luz mediante una fibra óptica entre los nodos comunicantes, o que exista visibilidad directa entre ambos nodos, una condición que no puede ser garantizada en todos los ambientes de trabajo. Además, los sensores ópticos requeridos generalmente no están presentes en los clientes y deben ser instalados separadamente.

Sin embargo, la transmisión sobre un canal acústico tiene como ventaja el poder utilizar hardware instalado en la mayoría de los potenciales clientes, tales como parlantes o micrófonos estándar, elementos comunes en dispositivos electrónicos masivos [76]. Además, no es necesaria la visibilidad directa mientras ambos nodos estén localizados a pocos metros de distancia.

En contraste con otras tecnologías como RF o enlaces ópticos, la naturaleza del

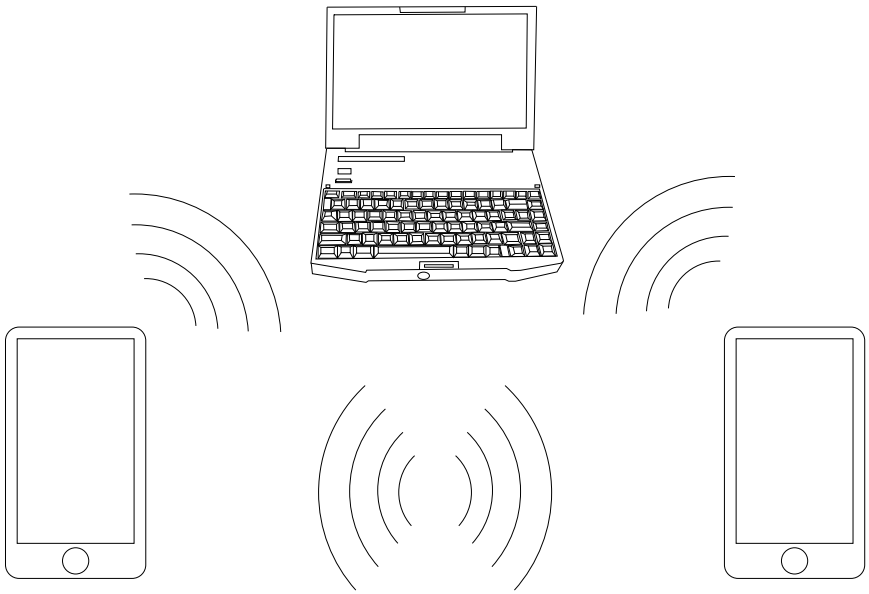


Figura 3.11: El diseño de red acústica propuesta puede contener nodos heterogéneos, tales como teléfonos del tipo smartphone o computadoras personales.

canal acústico y la facilidad para interceptar o registrar comunicaciones utilizando este medio hace de la privacidad un requerimiento esencial. Algunos sistemas de comunicación de audio han sido propuestos [77], pero el problema de la privacidad en este tipo de comunicaciones se soluciona generalmente en la capa de aplicación, es decir, en alto nivel. Esta Tesis presenta una aproximación a la seguridad y privacidad desde la capa física, basada también en time-hopping CDMA, similar a aquella presentada en [78]. Presentaremos una red segura acústica punto a punto y punto a multipunto de corto alcance y bajo consumo, que no requiere de ningún hardware adicional en clientes móviles.

Un escenario válido para la aplicación de esta tecnología podría ser validación de transacciones financieras pequeñas tales como terminales PoS *(Point of Sale)* o cajeros automáticos (ATM) utilizando un dispositivo móvil (por ejemplo, un celular del tipo *smartphone*) sin modificaciones de hardware. Una tecnología similar que se utiliza en estos casos es la denominada NFC *(Near Field Communications)* [79], un protocolo inalámbrico que requiere hardware especializado que, al momento presente, no se encuentra disponible en la mayoría de los dispositivos móviles. Con respecto a la implementación sobre el medio óptico, es necesario ajustar algunos parámetros,

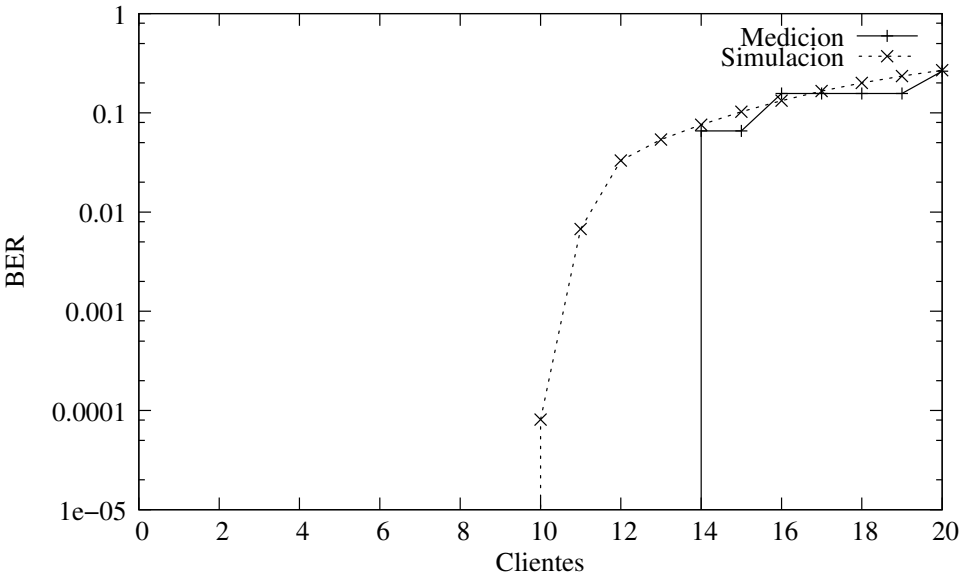



Figura 3.12: Simulación y medición del BER para una red acústica en función del número de clientes con M=256 y K=9.

como por ejemplo el tamaño de trama, que se reduce de $M = 4096$ a $M = 256$ para la implementación acústica, y el parámetro $K = 9$ que es el óptimo para el $M$ seleccionado. El número de clientes también se ve reducido de $N = 128$ a $N = 12$ ya que al ser la red acústica de corto alcance, no se prevé una elevada cantidad de clientes simultáneos. En la figura 3.12 se muestra una simulación del sistema con estos parámetros contrastada con una medición realizada entre una Notebook (T420) y un celular (Lenovo A789). En dicha figura se puede apreciar que las simulaciones y las mediciones son similares, mostrando estas últimas desde 14 clientes en adelante. La razón por la cual sólo se muestra a partir de 14 clientes reside en que la tasa efectiva de transmisión es muy baja y para medir un BER más grande, se necesitaban tiempos del orden de un día. Teniendo en cuenta que este tipo de sistemas se utilizarían para transacciones de pocos bytes, y la coincidencia entre la curva simulada y la real, consideramos que el desempeño es adecuado.

### 3.10.3 Redes acústicas: arquitectura

Una ventaja importante del sistema acústico propuesto es su simplicidad, requiriendo solamente un emisor de sonido (parlante), un receptor (micrófono) y un canal de

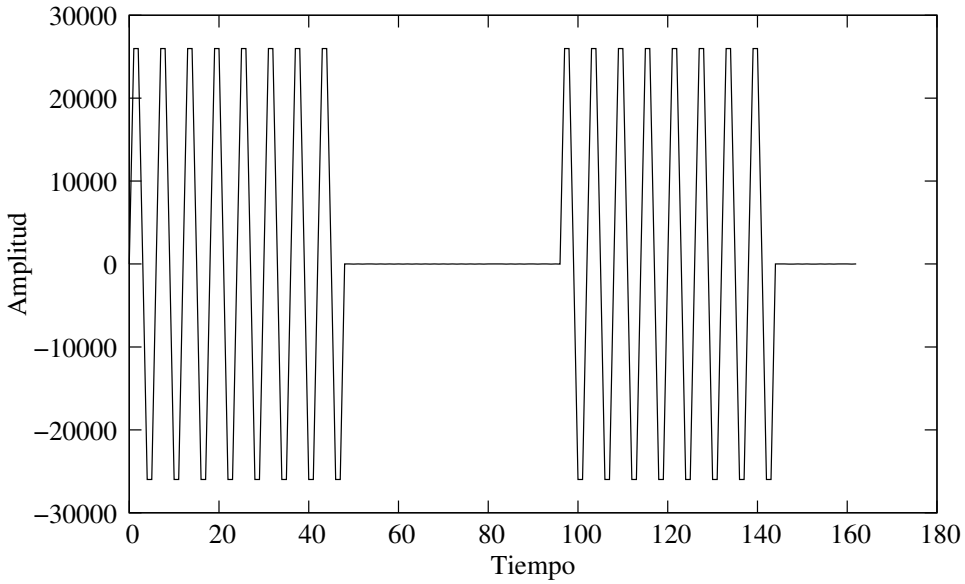



Figura 3.13: Modulación OOK.

transmisión de sonido que puede ser aire (y, en casos más especializados, agua). Ambos requerimientos están generalmente disponibles en computadoras, notebooks, tablets y teléfonos celulares. El esquema lógico es el mismo que el descrito anteriormente: time-hopping CDMA seguro, códigos correctores de errores y un método de sincronización a nivel de bit. Como resultado, el sistema soporta canales unidireccionales a los clientes que sirven tanto para comunicaciones punto a punto como punto a multipunto. Para la implementación de canales bidireccionales, pueden utilizarse dos canales separados (ej. utilizando dos códigos CDMA diferentes), o empleando el mismo canal de manera *half duplex*, aunque este último modo de funcionamiento necesita de desarrollo adicional y no es el objetivo de esta Tesis. En las próximas secciones se describe el sistema en mayor detalle.

### 3.10.4 Redes acústicas: modulación y sincronización

A diferencia de la implementación óptica donde se utilizaron algunas funciones provistas por el hardware de FPGA, tales como el mecanismo de sincronización de bit, para la transmisión acústica se implementaron tanto el algoritmo de modulación como el de sincronización totalmente en software. Para la modulación, fue utilizado el algoritmo de OOK (ver Fig. 3.13), que codifica los bits a transmitir como pulsos. La frecuencia

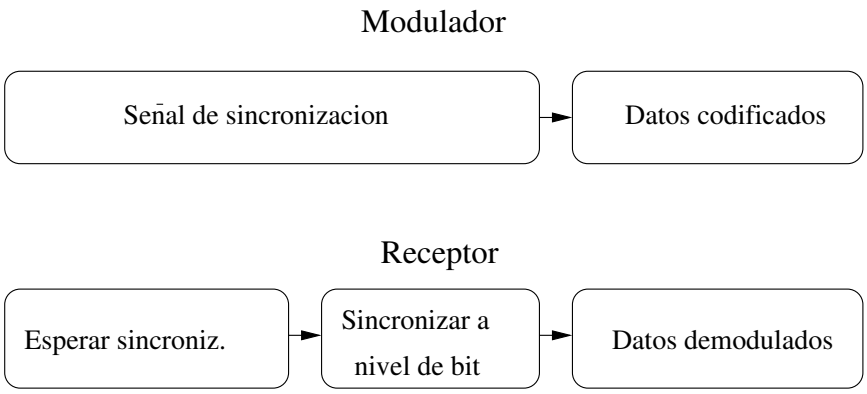



Figura 3.14: Sincronización.

de portadora puede variar de 10 kHz a 16 kHz, y la tasa de transmisión se fijo a 1000 bps. Debido a la baja velocidad de este canal se introduce un problema inexistente en la implementación óptica: el retraso de la red (el tiempo que tarda un bit en atravesar toda la red) es alto, debido principalmente a la etapa de Reed-Solomon que necesita recibir 256 bytes para comenzar el proceso de decodificación del bloque. Debido a que el canal soporta una velocidad máxima de 1000 bps, el retraso puede alcanzar niveles inaceptables, del orden de los 30 segundos. Una selección mas apropiada del algoritmo de FEC (tal como BCH) podría reducir reducir el retraso total del sistema. Adicionalmente, una etapa de *pulse shaping* o formación de pulso fue implementada, utilizando un filtro pasa-banda a la salida de la modulación y también en la entrada del demodulador. Este filtro ayuda a rechazar interferencia acústica o ruido ambiente.

La sincronización entre un transmisor y un receptor es esencial para la decodificación correcta de la información. Por esta razón, un patrón de sincronización inicial es enviado, para que el receptor pueda ajustar parámetros tales como la fase y nivel de decisión de la señal (ver Fig. 3.14). La deriva *(drift)* del reloj y variabilidad *(jitter)* no son significativas a esta baja velocidad de transmisión y ninguna corrección en tiempo real es requerida, por lo que la implementación del módem por software es simple. El nivel de decisión del demodulador es dinámico, es decir que es constantemente recalculado utilizando los niveles de entrada promediados. La fase del símbolo recibido también es corregida utilizando los mismos datos de entrada como referencia.

# Capítulo 4

# Resultados experimentales: medios de transmisión óptica y acústica

En este capítulo se muestran resultados numéricos y experimentales de la implementación del esquema de seguridad propuesto, para los diferentes módulos y el sistema completo, en medios de transmisión ópticos y acústicos.

## 4.1 Implementación en software

Como paso previo a realizar las implementaciones sobre FPGA en el caso óptico, y sobre software en el caso acústico, se implementaron simuladores numéricos de todas las etapas, y se combinaron para comparar los resultados con los teóricos. El simulador fue programado utilizando el lenguaje de C/C++. Fue necesario utilizar este tipo de lenguaje de alto rendimiento debido a que se necesitan simular grandes cantidades de datos para realizar mediciones de tasas de error del orden de 10e-8. Específicamente, en cada paso de simulación se transmite más de 1 Gb de datos por cliente, con hasta 128 clientes, por lo que se requiere del mayor rendimiento posible para obtener tiempos de ejecución aceptables.

### 4.1.1 Estructura general

La estructura general del simulador es modular, con una separación de alto nivel que obedece al diagrama lógico que puede verse en la figura 3.2. Cada módulo representa una etapa en el sistema de comunicaciones que realiza una transformación

específica sobre los datos, que puede ser modulación, demodulación, corrección de errores, etc. Los diferentes módulos actúan como filtros, recibiendo y enviando los datos transformados utilizando la entrada y salida estándar del sistema operativo (STDIN/STDOUT). La simulación comienza con un bloque generador de datos binarios aleatorios.

Estos datos son alimentados a la segunda etapa, que es el módulo de corrección de errores. La salida codificada de este módulo es posteriormente alimentada a la siguiente etapa, y de esta manera, los datos originales son sucesivamente transformados en cada módulo.

El medio de transmisión físico es también simulado mediante un modulo que simula las características físicas del canal seleccionado; por ejemplo, en el modulo de simulación óptica, se tienen en cuenta la dispersión y la atención de la señal introducidas por la fibra óptica.

Al llegar a la simulación de la última etapa de la recepción, donde deberían obtenerse los datos originales, el resultado es comparado bit a bit con los datos introducidos originalmente y, en base a las diferencias detectadas, se calcula y reporta el BER. Esta estructura modular brinda flexibilidad al simulador, permitiendo introducir y remover etapas fácilmente.

Sigue a continuación una lista de los módulos y sus características relevantes:

**rsenc/rsdec** Codificador/Decodificador de la etapa de corrección de errores. Específicamente, se implementa el algoritmo Reed-Solomon. Es posible generar un código "recortado" especificando la cantidad de bytes por bloque en el primer argumento.

**scrambler/descrambler** Implementación del scrambler de datos. El tamaño de bloque puede ser especificado en el primer argumento. Es recomendable que el tamaño de bloque sea un múltiplo del tamaño de bloque del corrector de errores (en nuestro caso, 255 bytes).

**bfenc/bfdec** Etapa codificadora/decodificadora que utiliza el filtro de Bloom. Para simular la interferencia en el medio compartido, en esta etapa se genera un flujo de datos aleatorio por cada cliente a simular y se lo agrega a la trama, lo que

provocará colisiones. El único argumento es la cantidad de clientes presentes en el canal.

**noisesim** Simulador de ruido óptico y de distorsión de la señal en la fibra óptica. La tasa de transmisión esta fija a 10 Gb/s. El único parámetro especifica la cantidad de clientes interfiriendo la señal.

**bin2wav/wav2bin** Modulador/Demodulador acústico. Transforma la señal de entrada en ondas acústicas con codificación PCM (*Pulse Coded Modulation*). El módulo de sincronización de audio se encuentra dentro de la utilidad wav2bin.

En general, el simulador puede ejecutar cada etapa consecutivamente, donde cada módulo completará el procesamiento de datos antes de comenzar con la próxima etapa:

```
./rsenc <${FILE} | ./scrambler ${SCRAMBLEBLOCK} >rs.out
./bfenc ${CLIENTES} < rs.out | ./noisesim -c ${CLIENTES} -r 16.6 >bfenc.out
./bfdec ${CLIENTES} <bfenc.out >bf.out
./descramble ${SCRAMBLEBLOCK} <bf.out | ./rsdec >rsdec.out
```

En el ejemplo anterior, los módulos utilizan archivos temporales como forma de comunicación. Esto causa que cada módulo deba finalizar el completo procesamiento de los datos de entrada antes de que sean procesados por el módulo siguiente.

Una simple modificación al ejemplo anterior permite prescindir del uso de archivos temporales, mediante la ejecución paralela:

```
./rsenc <${FILE} | ./scrambler ${SCRAMBLEBLOCK} | ./bfenc ${CLIENTES} | \
                ./noisesim -c ${CLIENTES} -r 16.6 | ./bfdec ${CLIENTES} | \
                ./descramble ${SCRAMBLEBLOCK} | ./rsdec > file.out
```

En la primera configuración del simulador se puede acceder a los archivos temporales intermedios, útiles para depuración y mediciones por etapa, mientras que la segunda configuración tiene la ventaja de aprovechar la totalidad de los procesadores

disponibles en el sistema, ya que en un sistema multiprocesador, el sistema operativo usualmente asigna un CPU a cada etapa y estas se ejecutan en paralelo.

La implementación sobre un medio acústico no presenta mayores inconvenientes con respecto a la velocidad de procesamiento, ya que las tasas de transmisión son bajas, acotadas naturalmente por el medio de transmisión y ancho de banda disponible, por lo que los recursos computacionales necesarios para la simulación son limitados. Utilizando el medio óptico, normalmente se necesita simular la transmisión de un gigabit o más para obtener una medición confiable del BER del sistema, ya que este medio tiene naturalmente una tasa de transmisión elevada y un BER pequeño, del orden de 10e-12. Adicionalmente, sobre este último medio el sistema soporta un máximo de 128 clientes que son simulados simultáneamente, por lo que los recursos computacionales requeridos son considerables. A raíz de este problema, y aprovechando que la simulación es altamente paralelizable, se implementó un sistema de estilo cliente-servidor donde los cálculos son distribuidos en un grupo de nodos.

### 4.1.2 Etapa de corrección de errores/scrambler

Los módulos de corrección de errores (rsdec/rsenc) fueron implementados utilizando bibliotecas de código abierto. Se utilizó la popular biblioteca libFEC del autor Phil Karn [62]. En cuanto al los módulos de scrambler/descrambler, se implementó un algoritmo de scrambling que utiliza una matriz de permutación aleatoria generada mediante una semilla en cada ejecución, garantizando que las permutaciones sean reversibles.

### 4.1.3 Implementación de filtro de Bloom

El módulo bfenc/bfdec realiza la codificación/decodificación por software del algoritmo de filtro de Bloom. Los parámetros del algoritmo, tales como el tamaño del filtro $M$ y la cantidad de clientes a simular, son configurables. Una característica que merece mencionarse es la del sistema de minimización de peso de Hamming que es

realizado en esta etapa. Tal como se explico en 3.5, la implementación se implementó mediante una tabla de lookup (ver tabla 3.1), lo que permite consultas muy eficientes con una complejidad temporal de $O(1)$, aunque el tamaño de la tabla (también llamado complejidad espacial del algoritmo) se aproxima a $O(2^N)$, donde $N$ es la cantidad de bits por símbolo, por lo que para tamaños razonables de $N < 24$, la tabla es autogenerada en cada ejecución en función de los parámetros necesarios.

### 4.1.4 Simulador de medio acústico

El medio de transmisión acústico fue simulado adoptando un modelo físico relativamente sencillo, que sólo toma en cuenta ciertas limitaciones en la respuesta en frecuencia. Para esto, se crearon módulos independientes que realizan la modulación, sincronización, demodulación y filtrado de la señal resultante. Los módulos transforman los bits de entrada en una señal de audio digital con codificación PCM, a la cual se aplica un filtro pasa banda para simular las limitaciones en frecuencia de los transductores, que comúnmente son son los parlantes y micrófonos de un dispositivo móvil. Este módulo respeta el diseño de los anteriores, emitiendo la señal analógica como un flujo de bytes con codificación PCM vía la salida estándar del sistema. El filtro pasa banda fue implementado como un filtro digital de respuesta finita o FIR *(Finite Impulse Response)*. Este simulador utiliza algoritmos de modulación, filtros y sincronización reales, por lo que muchos módulos pudieron ser reutilizados sin modificaciones en un medio real. Para más detalles, ver sección 4.4.

### 4.1.5 Simulador de ruido óptico

El modelo de simulación del canal óptico toma en cuenta tanto efectos lineales como no lineales en la fibra óptica.

Se asume que el tráfico proveniente de todas las ONUs alcanza al divisor de $128 \times 1$ con perfecta sincronización de bit y sin fluctuaciones o *jitter*. Los casilleros correspondientes al bit '0' contienen una pequeña intensidad óptica de CW (*Continous Wave*,

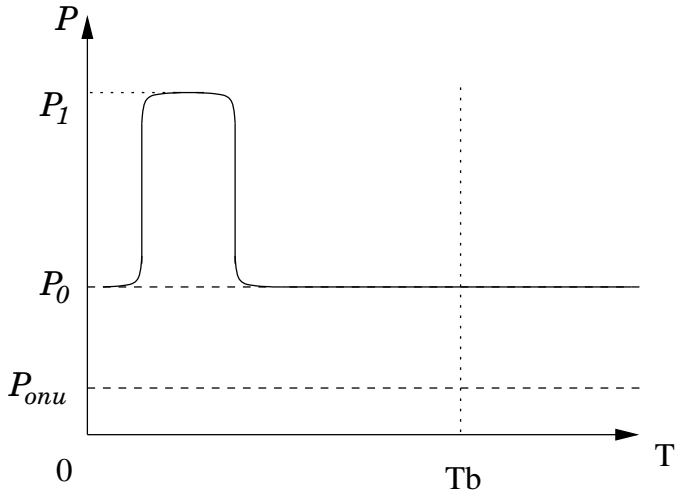



Figura 4.1: Diagrama de un bit supergaussiano (m=4) con ciclo útil de 1/4. La potencia del nivel del cero no equivale a potencia cero, sino a $P_0$, que se define como $P_0 = P_{ONU} * n$ donde $n$ es la cantidad ONUs activas, y $P_{onu}$ es la potencia generada cuando el láser emite el bit '0'.

potencia siempre presente en el láser) dada por el razón de extinción de Tx. Debido a esta potencia óptica siempre presente, cada ONU agregado al sistema agrega una pequeña intensidad de bit '0', incrementando la potencia base total (ver figura 4.1). Para la simulación se asume que cada bit '1' agrega un pulso super-Gaussiano ($m = 4$) al nivel de potencia base, con un ciclo de trabajo (*duty cycle*) de 1/3, una aproximación razonable a los parámetros utilizados por el transceptor multigigabit utilizado.

Tanto el tráfico saliente como el entrante sufren atenuaciones debido a múltiples factores que incluyen pérdidas en el divisor, fibra y empalme (*splice*). El presupuesto de potencia (*power budget*) se balancea mediante un EDFA (*erbium-dopped fibre amplifier*) con una ganancia constante de 27 dB, valor calculado como el necesario para compensar las pérdidas totales sobre un enlace de 10 Km. Un factor en el incremento del BER sobre enlaces ópticos es la emisión espontánea amplificada del EDFA. Este parámetro es modelado como ruido blanco gaussiano, con una intensidad proporcional a la figura de ruido del amplificador (7 dB), y es agregado luego del modelado del EDFA.

La señal de entrada óptica al receptor es filtrada con un filtro Butterworth de segundo orden y 25 GHz de ancho de banda, para luego simular su detección asumiendo la respuesta de un dispositivo PD (*photodiode*) estándar (ver sección 4.4.3 de [80]). Finalmente, para simular el ruido térmico y ruido de disparo o *shot*, se agrega un componente de ruido blanco gaussiano.

## 4.2 Redes ópticas

La implementación del sistema sobre redes ópticas fue el objetivo principal de la investigación. La simulación tuvo un papel muy importante en el desarrollo y pruebas del algoritmo en este medio debido a las elevadas tasas de transmisión involucradas (el transceptor utilizado puede utilizarse a un mínimo de 1 Gbps y máximo de 9.33 Gbps), cuya observación y medición directa no es sencilla. Sin embargo, parámetros tales como el ancho de bit y relación de extinción pueden obtenerse fácilmente mediante el diagrama de ojo de la señal.

### 4.2.1 Simulaciones numéricas

Podemos citar dos resultados importantes obtenidos mediante las simulaciones numéricas. En el primero, detallado en la Fig. 4.2, se muestra que la razón de extinción mínima requerida para lograr un BER arbitrario es directamente proporcional al número de ONUs presentes on-line. Podemos deducir de este gráfico que mientras más ONUs utilicen el sistema, se necesitarán emisores lásers con una razón de extinción mas elevada. Además, con una mayor cantidad de ONUs, se incrementa el BER por problemas físicos: las fluctuaciones de niveles de potencia cercanos al límite de sensibilidad del dispositivo PD tienen un importante efecto en la detección de la señal. El ruido de shot o disparo es particularmente preocupante ya que es proporcional a la fotocorriente media. En nuestra propuesta, este ruido es más alto que en PONs comunes ya que la intensidad del bit '0' de todas las ONUs presentes contribuyen al mismo. En el escenario de 128 ONUs presentes, un BER menor a 10e-3 puede

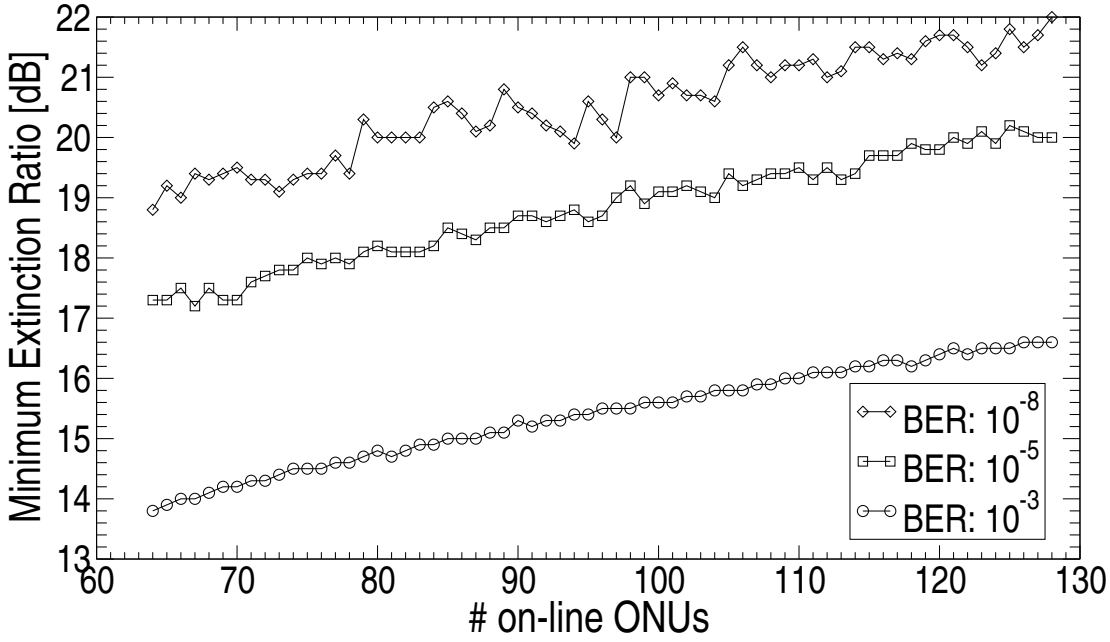



Figura 4.2: Resultado de simulaciones de la capa física: razón de extinción mínima requerida para asegurar un cierto BER.

ser logrado utilizando transmisores del tipo comercial con una razón de extinción de $\simeq$ 16,6 dB. Este BER es lo suficientemente bajo para permitir rutinas de corrección de errores al nivel del canal lógico, que garanticen la transmisión libre de errores con una utilización acotada de la capacidad total del canal.

La Fig. 4.3 muestra los resultados de la simulación del canal, comparando el BER de un ONU con respecto al número total de ONUs activos. Las dos primeras gráficas muestran la diferencia en rendimiento al utilizar símbolos de 8 bits con respecto a símbolos de 16 bits y, en la tercera gráfica se aprecia el aumento en el BER como resultado de agregar una etapa de ruido óptico a la simulación. Los resultados fueron obtenidos enviando exactamente un gigabit de datos por cada ONU simultáneamente. El mismo método se utilizó para realizar las simulaciones cuyo resultados se presentan en la Fig. 3.8, donde se observa una mejora de rendimiento importante al utilizar el algoritmo de reducción de peso de Hamming. Volviendo a la Fig. 4.3, puede verse que cuando la cantidad de ONUs supera los 128, el BER se eleva marcadamente. De la

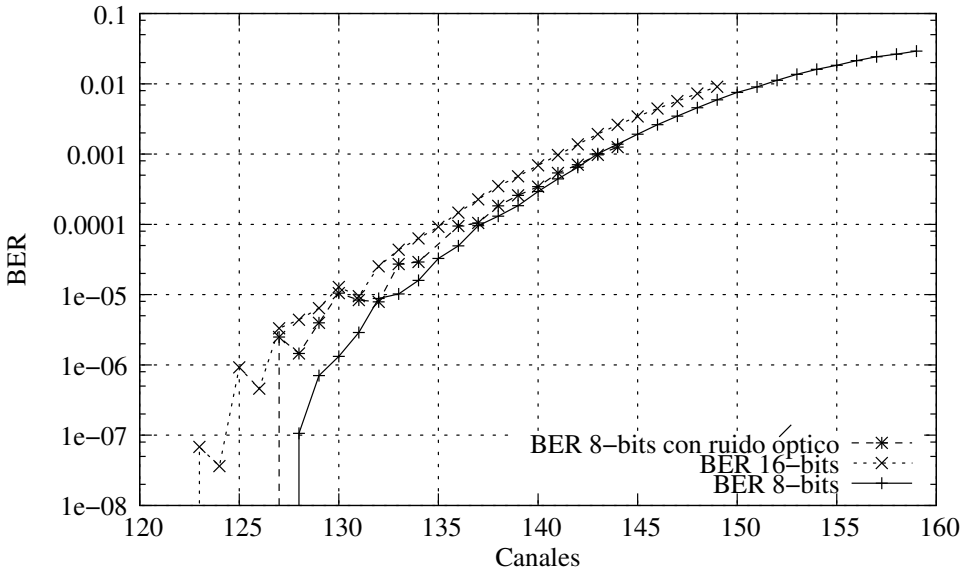



Figura 4.3: BER del canal de un ONU a 10 Gbps vs. la cantidad de ONUs activos. La curva de "BER 16 bits" utiliza símbolos de 16-bits. Tiene mejor performance que la curva "BER 8 bits" con símbolos de 8 bits. Finalmente, si simulamos el ruido óptico del canal, la performance disminuye ligeramente como puede verse en la curva "BER 8 bits con ruido óptico".

misma figura podemos observar una disminución de la capacidad en aproximadamente 8 ONUs cuando el ruido de la capa óptica es agregado a la simulación, debido a la razón de extinción y el ruido producido por el EDFA y los PDs. Finalmente, la carga máxima que soporta el sistema con un BER de 10e-8 es del 90 %, lo que significa que en una red de 128 clientes, pueden transmitir simultáneamente hasta 119 ONUs.

## 4.3 Implementación en FPGA

El estudio de PONs plantea el desafío de generar, transmitir y recibir señales de 10 Gbps en el laboratorio. El costo de estos sistemas suele ser muy elevado. Uno de los objetivos de esta tesis es presentar una alternativa de muy bajo costo basada en la generación y trasmisión de señales ópticas utilizando dispositivos del tipo FPGA.

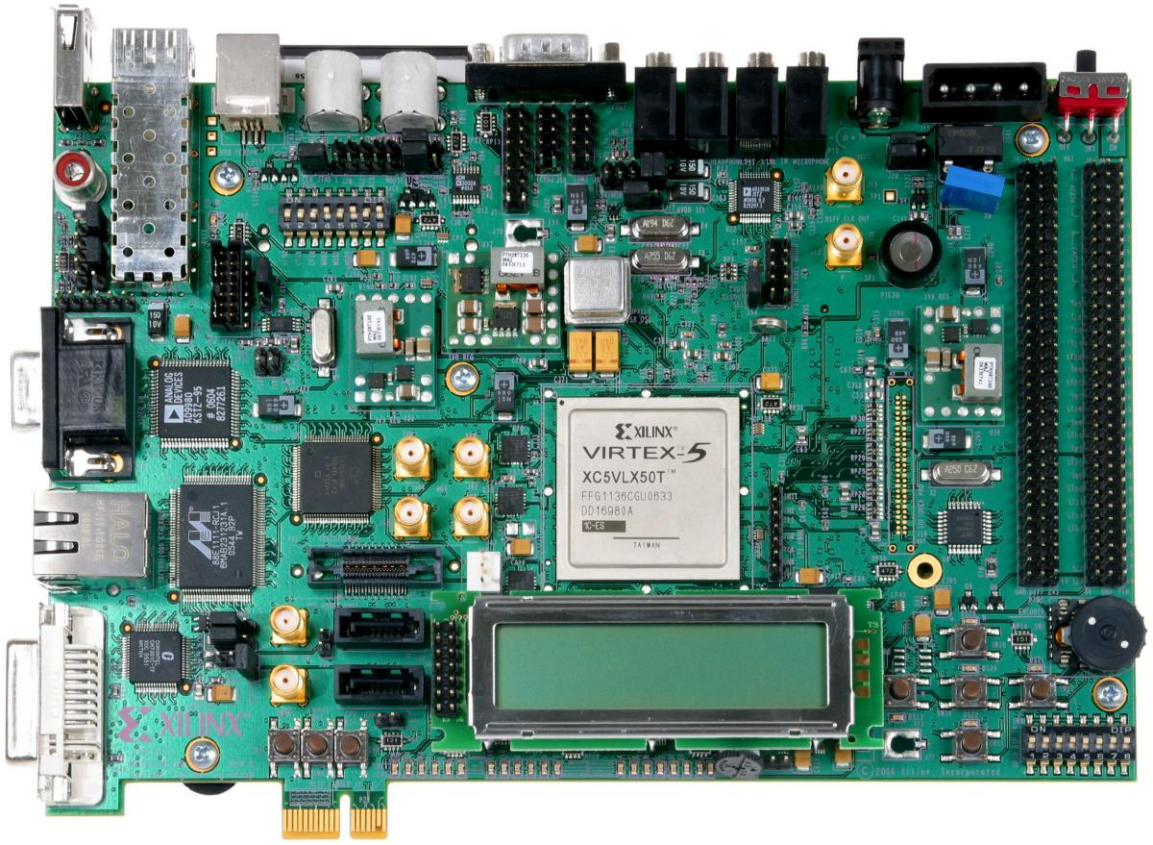



Figura 4.4: Placa de desarrollo ML570 de Xilinx. Los conectores utilizados son: 1: SFP+, 2: JTAG, 3: alimentación +5V, 4: Switch on/off, 5: Interfaz serial RS232, 6: salida de reloj.

### 4.3.1 Arquitectura alto nivel de la FPGA Xilinx ML507

El equipo se compone de un kit de desarrollo ML-507 de Xilinx [81] (ver figura 4.4) y un transceptor óptico con varios emisores láser con longitudes de onda de 1330 nm y 1550 nm, ambos con capacidad de hasta 10 Gbps en modulación NRZ y alcance de 10km en fibra monomodo [82]. Para realizar las mediciones se utilizaron dos herramientas de medición:

- Osciloscopio óptico Agilent 86100A con módulo óptico 86105A: para realizar las mediciones físicas contamos con este equipo que posee un ancho de banda en el módulo óptico de 20 Ghz, suficiente para capturar en tiempo real los bits individuales o realizar un diagrama de ojo.

- *Integrated Bit Error Rate Tester* (iBERT) [83]: este dispositivo es un medidor de tasa de error con interfaz para la herramienta de verificación y depuración ChipScope [84]. Esta herramienta puede denominarse "virtual" ya que consiste íntegramente en núcleos IP (*intellectual property*) puramente lógicos, que deben ser sintetizados y embebidos junto con el diseño dentro de la FPGA. Con iBERT es posible medir en tiempo real varios parámetros del transceptor, así como realizar estadísticas y mediciones de error, variando tasas y características de la transmisión en tiempo real.

### 4.3.2 Tranceptores multigigabit

La plataforma de FPGA de Xilinx no fue seleccionada solamente para utilizar la capacidad de procesamiento de la lógica programable para transmisión de datos a altas velocidades, sino por la versatilidad y velocidad de los transceptores multigigabit incluidos en las mismas, esto es, la "maquinaria" necesaria para serializar/des-serializar y codificar bits de datos a muy alta velocidad, así como las interfaces para conectar las salidas eléctricas directamente a las entradas de transceptores ópticos, como uno o más SFPs [85] (ver figura 4.4, punto 1). Es necesario mencionar que no existe razón técnica para utilizar un proovedor de FPGAs en particular, ya que muchos proovedores de FPGAs, como por ejemplo Altera [86], venden dispositivos de similares características y precio que Xilinx.

Los transceptores multigigabit están preparados para operar en diversos medios físicos como, por ejemplo, cables trenzados de cobre o líneas de transmisión de alta velocidad sobre PCBs (*printed circuit boards*). Serial-ATA [87] y PCI-Express [88] son protocolos de transmisión de datos que suelen ser implementados utilizando los transceptores de la FPGA. Sin embargo, en redes de comunicaciones PON, además de funcionar a tasas transmisión multigigabit se necesitan alcances del orden de kilómetros, características que suelen requerir un medio de transmisión que utiliza fibras ópticas. El transceptor posee varios módulos adicionales como, por ejemplo, un sistema de sincronización por hardware, sistemas de recuperación de reloj y la capacidad

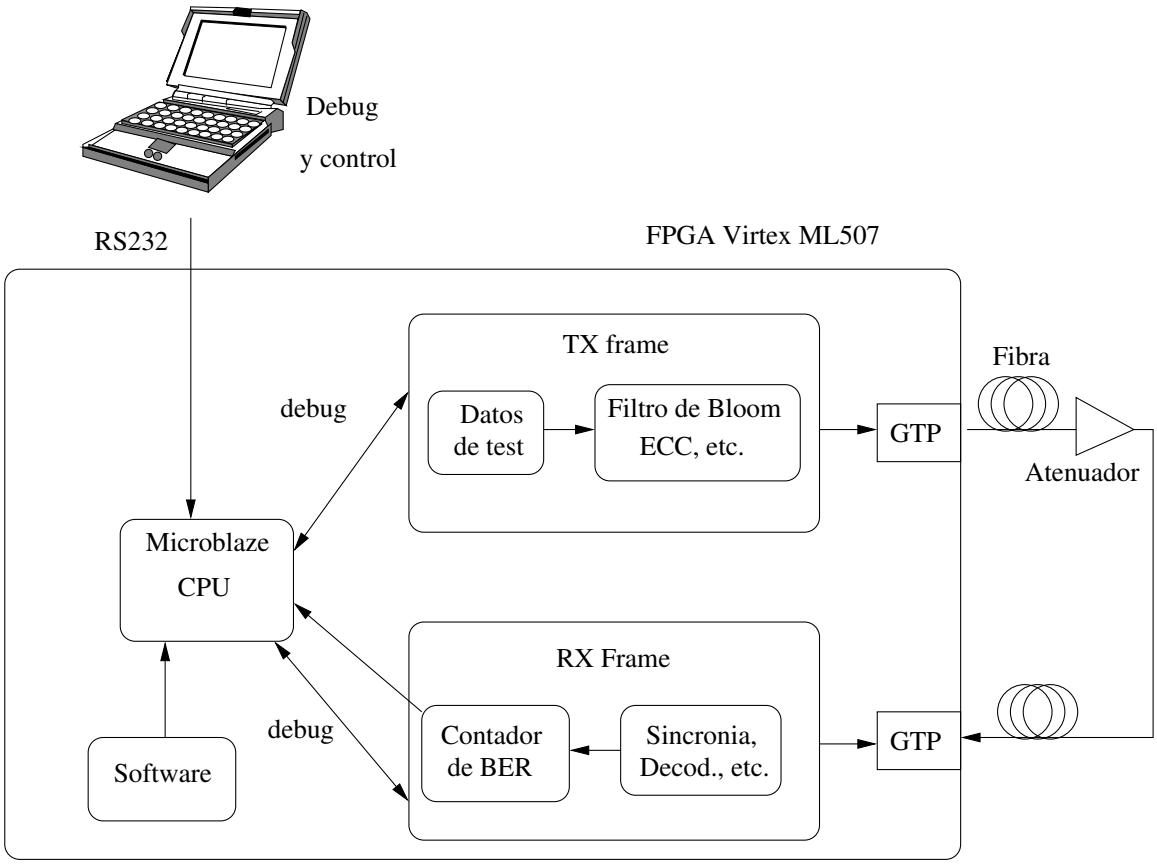



Figura 4.5: Diseño lógico de alto nivel sobre FPGA

de realizar una codificación 8B/10B [89] adicional, con el objetivo de mantener el balance de DC (*direct current*), pero este último módulo fue desactivado ya que interfiere con los demás codificaciones (para una explicación mas detallada, ver sección 4.3.7).

### 4.3.3 Diseño digital del sistema propuesto

En la Fig. 4.5 puede observarse el diseño digital propuesto en el cual se implementó y probó exitosamente el algoritmo transmitiendo a tasas de 5 Gigabits mediante una fibra óptica. Estas velocidades fueron logradas gracias a ciertas características del diseño que serán descritas a continuación. En la Fig. 4.6 se muestra el diseño digital o de hardware. En esta figura, puede verse que el sistema se compone de dos módulos principales: el CPU que actúa de módulo de control y el coprocesador de

comunicaciones. El diseño fue realizado íntegramente para la Tesis, y puede manejar tasas de 5 Gbps con un reloj del sistema de sólo 75 Mhz.

El módulo de control cumple la función de interfaz entre el sistema y el usuario, permitiendo modificar parámetros de manera sencilla y presentar las estadísticas de una manera rápida. Se presenta al usuario como un sistema de menús en modo texto, mediante los cuales el operador puede ejecutar comandos y leer valores del sistema. La interfaz al usuario se realiza a través de un puerto serial del tipo RS-232. Para su implementación se utilizó un soft-CPU (CPU sintetizado dentro de la misma FPGA) del tipo Xilinx Microblaze [90], y un programa en lenguaje C encargado de imprimir los menús de control y enviar y recibir datos hacia los módulos generadores y decodificadores de trama. Las operaciones se realizan de manera asincrónica con el resto del hardware, por lo que la velocidad de reloj del CPU puede ser muy reducida. Este módulo se implementa en el archivo "copro1.v" que también es el módulo principal del diseño, interconectando las señales de todos los submódulos de generación y decodificación de tramas.

El coprocesador de comunicaciones puede separarse en cuatro sub-módulos:

**Transceptor multigigabit:** este componente de hardware es provisto por la FPGA. Puede pensarse en alto nivel como un serializador/deserializador (SERDES), pero contiene más de 15 subsistemas, incluyendo buffers, PLLs (*phase-locked loop*), codificadores y decodificadores. Adicionalmente, el transceptor posee herramientas para sincronización y depuración, permitiendo realizar mediciones y crear lazos de realimentación o *loopbacks* en tres puntos diferentes del flujo de datos para detectar anomalías. Se conecta a la lógica programable de la FPGA por medio de más de 200 señales de control y transferencia de datos, cuyas funciones son encapsuladas por un módulo especial de lógica, que simplifica la interfaz con el resto del sistema. Esta lógica de interfaz se implementó como un módulo de Verilog, llamado "v5_gtxwizard_v1_7_tile.v" en el código fuente.

**Generador de trama:** este módulo se encarga de codificar los datos a transmitir y

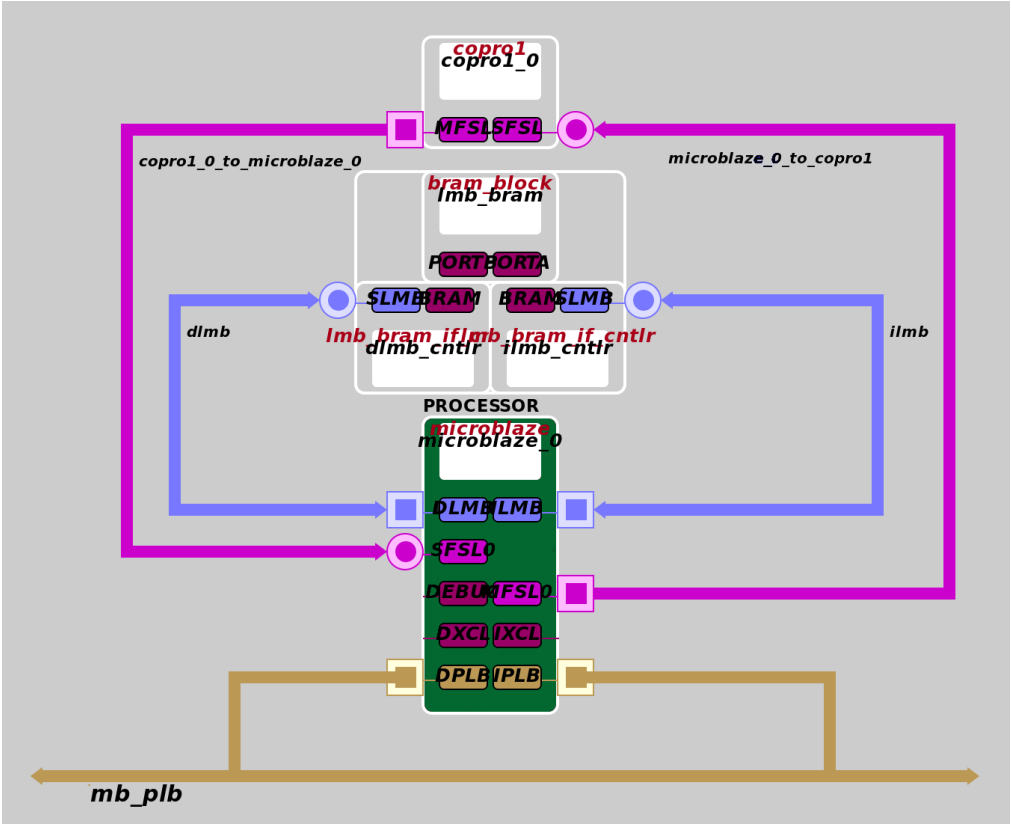
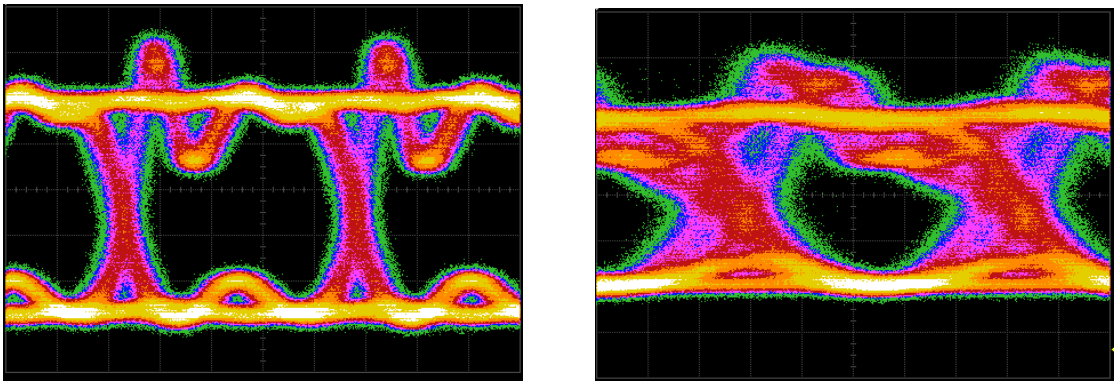



Figura 4.6: Diseño de hardware sobre la FPGA: se aprecian los módulos principales, siendo copro1 el coprocesador de comunicaciones. microblaze_0 es el CPU y bram_block es el bloque de memoria utilizado por el CPU, conectado al mismo mediante dos buses: dlmb y ilmb, buses de datos e instrucciones del tipo LMB (*local memory bus*). El coprocesador se conecta mediantes dos buses, llamados copro1_0_to_microblaze_0 y microblaze_0_to_copro1, ambos buses del tipo FSL (*fast simplex link*). Finalmente, el CPU se conecta a los periféricos como RS232 y switches por medio del bus mb_plb, del tipo PLB (*peripheral local bus).*

enviarlos por el transceptor multigigabit. Contiene implementaciones de todas las etapas necesarias, tales como el codificador de ARC4, Bloomfilter encriptado y expansión de peso de Hamming, así como también el sistema de sincronización de trama. La estructura interna es la de una máquina de estados finita, estando implementada íntegramente en lógica digital (sin utilizar ningún componente de software). Se implementó en un sólo módulo de Verilog llamado “frame_gen.v”.

**Decodificador de trama:** la contrapartida del generador de trama es el decodificador, que posee los decodificadores correspondientes tales como Reed-Solomon, ARC4, Bloomfilter, expansión de peso de Hamming y finalmente el sincronizador de trama, que utiliza parcialmente el hardware de sincronización del transceptor multigigabit para ajustar los tiempos de recepción a nivel de byte, sumado a una sincronización propia para lograr ajustes a nivel de double-word y finalmente, sincronización de la trama (ver sección 4.3.8). En lugar de un diseño convencional del tipo CPU+memoria, el diseño de este módulo consiste en una máquina de estados finitos implementada puramente utilizando elementos lógicos de la FPGA. Se implementó en un sólo módulo de Verilog llamado "frame_dec.v". Adicionalmente, un contador de BER se implementó en esta fase, dado que los datos enviados son un patrón de prueba y es posible medir la tasa de errores de manera simple. Las estadísticas de errores son exportadas mediante señales conectadas al módulo de control.

El sistema utiliza buffers tanto de lectura como de escritura al transceptor, por lo que puede operar a velocidades de reloj mucho menores. Por ejemplo, si el transceptor multigigabit posee un ancho máximo de bus TXDATAWIDTH y la velocidad de transferencia es TXCLOCK, la velocidad de reloj DATACLOCK necesaria para mantener los buffers internos del transceptor llenos es simplemente $DATACLOCK = TXCLOCK/TXDATAWIDTH$, por lo que transmitiendo a 5 Gbps utilizando el máximo TXDATAWIDTH de 32 bits, tenemos que $DATACLOCK = 156Mhz$ un valor alcanzable para la FPGA utilizada y fácilmente implementable en un futuro diseño de ASIC (*application-specific integrated circuit*). La velocidad de las implementaciones de generador CSPRNG ARC4 y el codificador/decodificador de Reed-Solomon son críticas para la performance del sistema ya que el resto de las etapas no introducen mayores retrasos. El algoritmo ARC4 fue implementado en Verilog poniendo especial énfasis en la performance, logrando un flujo de salida de un byte pseudoaleatorio por cada ciclo de reloj. Para el algoritmo Reed-Solomon se utilizó un IP de la biblioteca



(a) Tasa de 4,5 Gbps, 50ns por división.

(b) Tasa de 7,5 Gbps, 20ns por división.

Figura 4.7: Diagramas de ojo de la señal óptica a la salida de la fibra. Se observa una degradación importante de la calidad de la señal al aumentar la tasa de bits.

de Xilinx que tiene una performance óptima. Exceptuando este último algoritmo de Reed-Solomon, todo el resto del sistema fue implementado desde cero.

### 4.3.4 Transmisión a 9 Gbps con SFP+

La norma SFP+ [91] (*enhanced small form-factor pluggable*) especifica las dimensiones físicas y conectores eléctricos del transceptor óptico. Permite velocidades de hasta 16 Gbit/s y es el formato de transceptor utilizado en la mayoría de los kits de desarrollo de FPGA comerciales actuales. El transceptor SFP+ consta básicamente de un emisor láser, un detector y circutos ser-des (serializadores/deserializadores). El montaje para la experiencia se realizó conectando un transceptor SFP+ (ver figura 4.4, punto 1) con un láser de 1550 nm al conector correspondiente en la placa de desarrollo ML-507 y un bucle de fibra óptica (*loopback*), con el objetivo de realizar las mediciones de BER. Adicionalmente, generamos el disparo del osciloscopio mediante la señal eléctrica de reloj del sistema que se obtiene a través de los conectores SMA con código J12 y J13 (ver figura 4.4, punto 6). Al disparar el osciloscopio con la señal de reloj sincronizada con la señal de salida, podemos obtener el diagrama de ojo de la señal (ver figura 4.7).

Para la depuración y configuración se utilizó la interfaz JTAG USB de Xilinx

"Platform Cable USB II" [92] (ver figura 4.4, punto 2).

### 4.3.5 Configuración del reloj del transceptor

La tasa de transmisión del transceptor GTX está dada por la frecuencia de reloj de entrada $F_{PLL\_Clock}$, donde se transmite un bit por cada semiciclo (la modulación es NRZ); entonces, la tasa de transmisión será $R_{line}[\text{bps}] = F_{PLL\_Clock}[\frac{1}{s}] \times 2$. La frecuencia del reloj de entrada del PLL está especificada por la ecuación 5-1 [85]:

$$F_{PLL\_Clock} = F_{CLKIN} \times \frac{PLL\_DIVSEL\_FB \times DIV}{PLL\_DIVSEL\_REF}. \tag{4.1}$$

donde las constantes $PLL\_DIVSEL\_REF = \{1; 2\}$, $DIV = \{4; 5\}$ y $PLL\_DIVSEL\_FB = \{1; 2; 3; 4; 5\}$ son configurables por software; y la frecuencia base del PLL se configura con el switch físico SW6 [93, Tabla 1-32].

Modificando los parámetros puede lograrse, en teoría, un amplio rango de frecuencias $F_{PLL\_Clock}$, pero de acuerdo a la documentación del PLL [94, Pág. 71], este tiene un rango de operación nominal desde 1,2 a 2,7 Ghz. Sin embargo, es posible [95] la obtención y medición de velocidades de oscilación estables para el PLL de hasta 4,5 Ghz (lo que implica una tasa de transmisión de 9 Gbps), fuera del rango de operación especificado por el fabricante.

### 4.3.6 Características del transceptor multigigabit a altas velocidades

La Fig. 4.9 muestra la evolución de la señal óptica producida a diferentes tasas. Según la documentación del tranceptor [85], la máxima velocidad de transmisión es de 6,5 Gbps. Sin embargo, en la figura se observan mediciones a tasas mucho mayores, de hasta 12,44 Gbps. Esto obedece a dos razones:

- Es posible transmitir y recibir datos hasta una tasa de 9.33 Gbps, si en lugar de utilizar el procesador de la FPGA para realizar las mediciones, se utiliza el

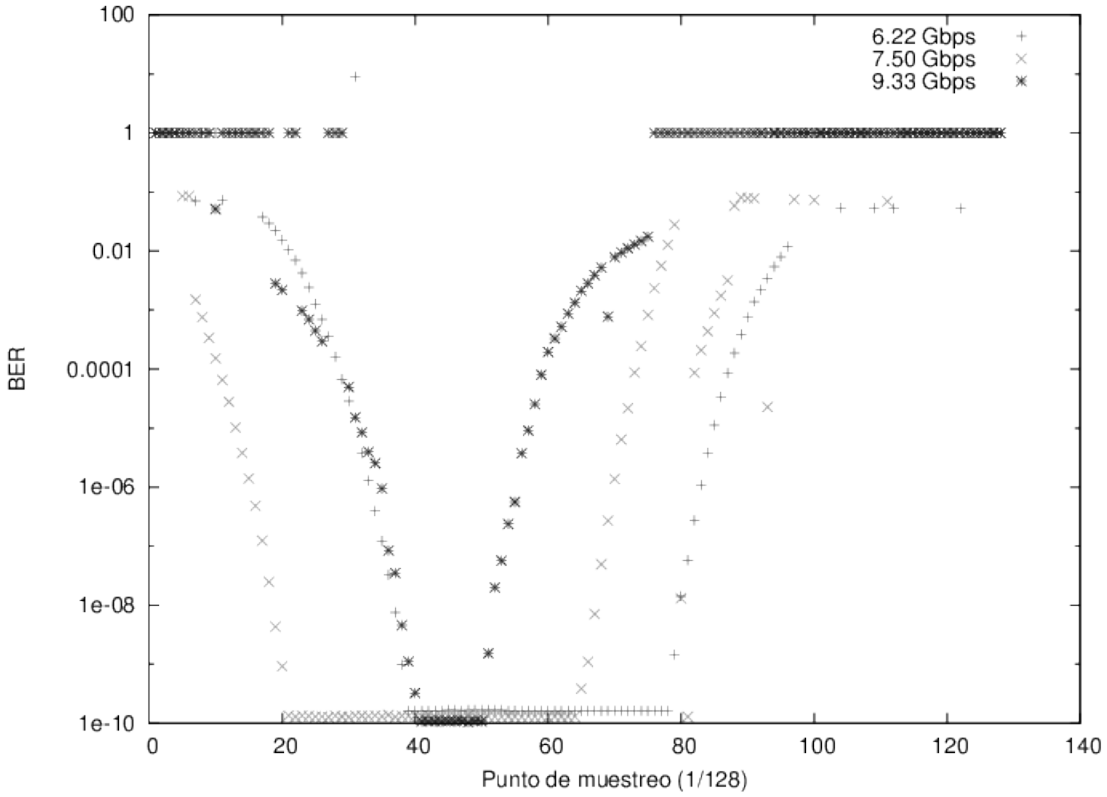
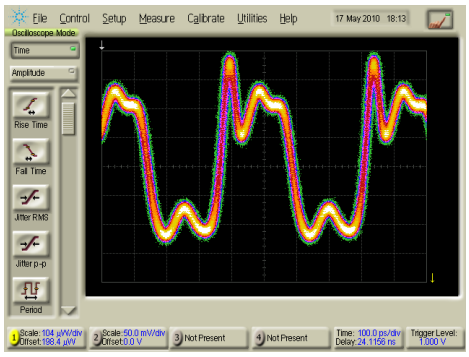



Figura 4.8: BER vs. punto de muestreo: la FPGA permite muestrear el valor del bit en 128 puntos equidistantes dentro del tiempo de bit. El BER aumenta cuando el punto de muestreo esta cerca de los extremos del bit (valores 0 y 128), donde el diagrama de ojo es más cerrado. Los diagramas de ojo pueden verse en la Fig. 4.7.

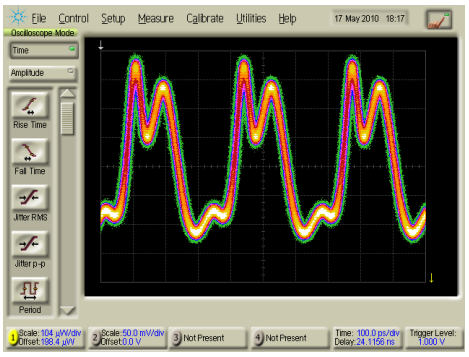
contador interno del transceptor. Esto es, los datos no son generados ni contabilizados por la FPGA, sino por circuitos de testeo dentro del mismo tranceptor, por lo que es posible alcanzar tasas mayores.

- Si eliminamos la necesidad de recibir y contabilizar los datos, el transceptor puede generar señales de hasta 12,44 Gbps. A estas tasas el transceptor sólo puede ser utilizado como un generador de señales, ya que no es posible realizar mediciones de BER. Un estudio más detallado de estos métodos puede verse en [95].

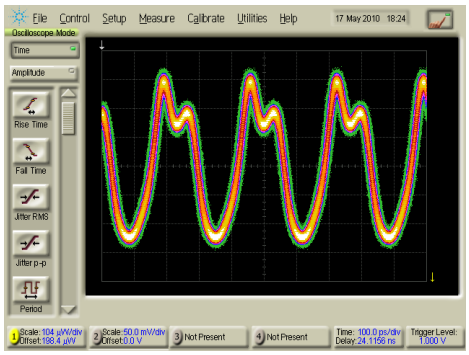
Todas las señales en la Fig. 4.9 corresponden a una transmisión de la secuencia 10101010, excepto la última figura, que fue generada con una secuencia distinta para



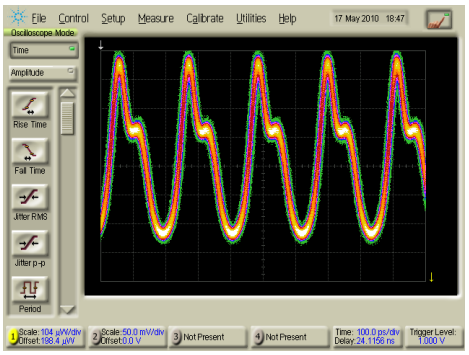

(a) Señal óptica a 4,5 Gbps



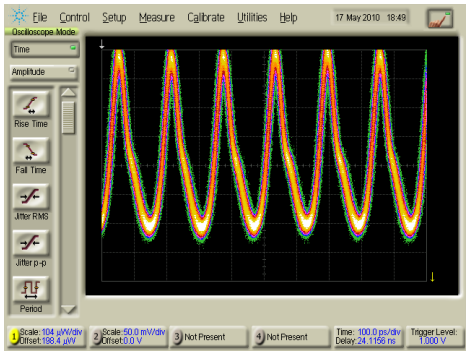

(b) Señal óptica a 6 Gbps



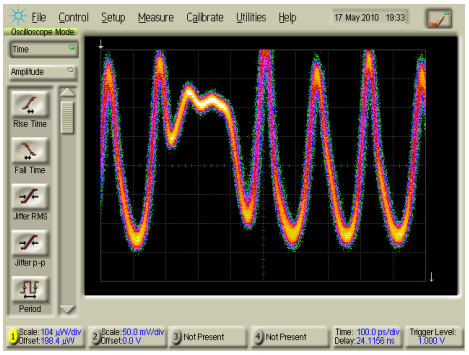

(c) Señal óptica a 7,5 Gbps




(d) Señal óptica a 9,33 Gbps




(e) Señal óptica a 12,44 Gbps




(f) Señal óptica a 12,44 Gbps, transmisión 10110101010

Figura 4.9: Medición de la señal óptica variando la tasa de transmisión de 4,5 Gbps a 12,44 Gbps. Se debe tener en cuenta que la señal será distorsionada debido al ancho de banda máximo del módulo de entrada óptico del osciloscopio, que es de 20 Ghz. La secuencia de bits enviada en todas las figuras es “1010101010” excepto en la figura f, donde es “10110101010”.

demostrar el control sobre la señal generada.

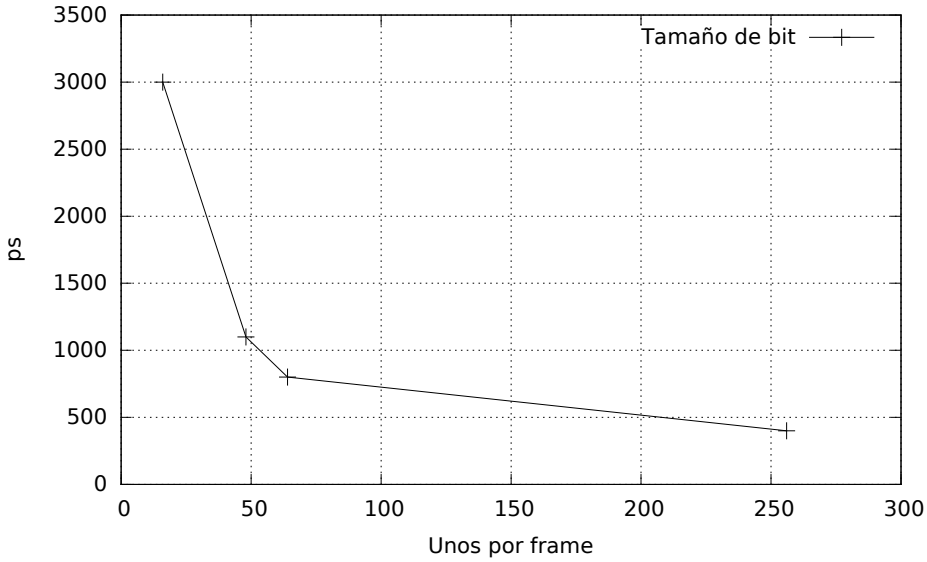
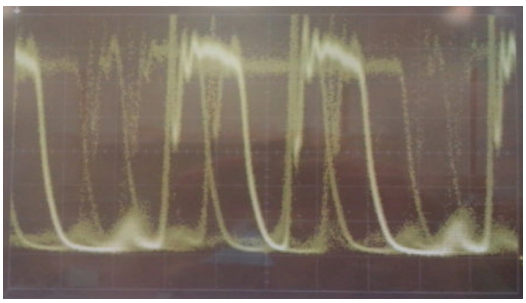



Figura 4.10: Se detalla la expansión del tiempo de bit (en picosegundos) en una señal desbalanceada a medida que la cantidad de unos por trama va disminuyendo. El tamaño de trama es de 512 bits, la tasa nominal es 2.5 Gbps y la duracion del bit es de 400ps.

Para determinar el valor del bit, el circuito receptor muestrea la señal de entrada en un punto determinado dentro del casillero o tiempo de bit. Este punto de muestreo de la señal es importante, ya que si se elige correctamente se minimizará el BER, tal como lo muestra la Fig. 4.8, donde se aprecia como el BER es minimizado si el punto de muestreo se encuentra aproximadamente en la mitad del tiempo de bit. Como puede verse en las Figs. 4.7, a tasas elevadas el pulso del bit se deforma y el punto de muestreo óptimo se modifica.

### 4.3.7 Problema de línea desbalanceada y codificación 8B/10B

La conexión eléctrica de la FPGA al módulo láser SFP+ se compone de 4 pares diferenciales, que deben transportar señales de hasta 4 GHz. En amplificadores eléctricos de alta velocidad, es deseable que la señal esté balanceada para obtener un componente nulo de corriente continua y poder acotar el ancho de banda necesario. Adicionalmente, una codificación donde se garanticen las transiciones de nivel cada un determinado número de bits, elimina el requerimiento de relojes de alta precisión en



(a) Señal con 256 bits en uno por trama (8B/10B), 400 ps por bit

(b) Señal con 48 bits en uno por trama, 1100 ps por bit

Figura 4.11: Señal de potencia óptica de un Láser SPF+ Sumitomo de 1330 nm. Se observa una expansión de bit cuando se reduce la cantidad de unos por trama, desbalanceando la señal. La tasa nominal utilizada para estas mediciones es de 2.5 Gbps

ambos lados de la línea de transmisión, ya que el reloj receptor puede re-sincronizarse utilizando dichas transiciones. Esto se logra mediante el denominado circuito de recuperación de reloj. Uno de estos algoritmos de balanceo es el denominado 8B/10B aunque existen otras codificaciones mas complejas. El transceptor multigigabit de Xilinx tiene un módulo de hardware interno que soporta codificación y decodificación 8B/10B automática de los datos de salida y entrada.

Sin embargo, esta codificación es incompatible con la implementación del algoritmo diseñado sin realizar modificaciones. Si se elimina esta codificación, la señal se degrada tal como se muestra en la Fig. 4.10, donde mediante mediciones directas con el osciloscopio óptico se aprecia una expansión progresiva del ancho de bit a medida que el desbalanceo de la señal se hace más pronunciado. Los efectos de la expansión del tamaño de bit son evidentes en la fig. 4.11 donde las gráficas de potencia óptica ponen en evidencia la expansión e interferencia causada por una señal desbalanceada. Efectivamente, el receptor recibe hasta 3 “unos” por cada “uno” transmitido de manera desbalanceada, generando una interferencia que impide el funcionamiento del sistema.

Este desbalanceo se soluciona simplemente aplicando las codificaciones a los datos antes de transmitirlos, tales como 8B/10B. Sin embargo, esta transformación es

incompatible con el filtro de Bloom, ya que la interferencia de dos señales basta para eliminar la codificación y desbalancear nuevamente la señal. Una posible solución sería utilizar un circuito de transmisión eléctrico compatible con señales desbalanceadas. Para el prototipo se utilizó otra solución, con el objetivo de utilizar la placa ML507 sin modificaciones y poder realizar mediciones sobre el protocolo: en el prototipo, uno de los clientes transmite su señal encriptada normalmente, mientras que los demás clientes son simulados mediante un patrón aleatorio pero balanceado eléctricamente, por lo que la señal es transmitida y recibida correctamente. La señal de estos clientes simulados no puede recuperarse, pero las mediciones son solamente realizadas sobre el cliente real, por lo que el sistema puede funcionar a la máxima tasa soportada por la FPGA (hasta 5 Gbps). El cliente real, al no estar codificado como 8B/10B, introduce un pequeño desbalanceo eléctrico que la línea de transmisión es capaz de soportar sin inconvenientes.

### 4.3.8 Sincronización a nivel de bit, word y trama

La sincronización no se trató detenidamente en la sección teórica de esta Tesis ya que desde un principio se consideró como un tema ajeno a la misma. Sin embargo, para la implementación final es imprescindible obtener la sincronización entre los nodos que deseen utilizar un canal. Esto no es una tarea sencilla considerando que debe hacerse sobre un canal que contiene una baja relación señal-ruido.

La estrategia utilizada para la transmisión por el medio óptico es utilizar el hardware de sincronización que posee el transceptor multigigabit ya incluido en la FPGA. Este módulo [85] denominado "*Comma Alignment and Detection*" se basa en la utilización de un prefijo o coma configurable que se compone de una serie de bits (que pueden tener 14 o 20 bits de largo en transceptores de tipo GTX) que se transmite cada vez que se desea sincronizar la etapa RX (receptor) con la TX (transmisor). Esta serie de bits es configurable pero es deseable que posea ciertas características, tales como una alta autocorrelación, para optimizar su detección en el flujo de datos recibidos. La sincronización se realiza en dos etapas:

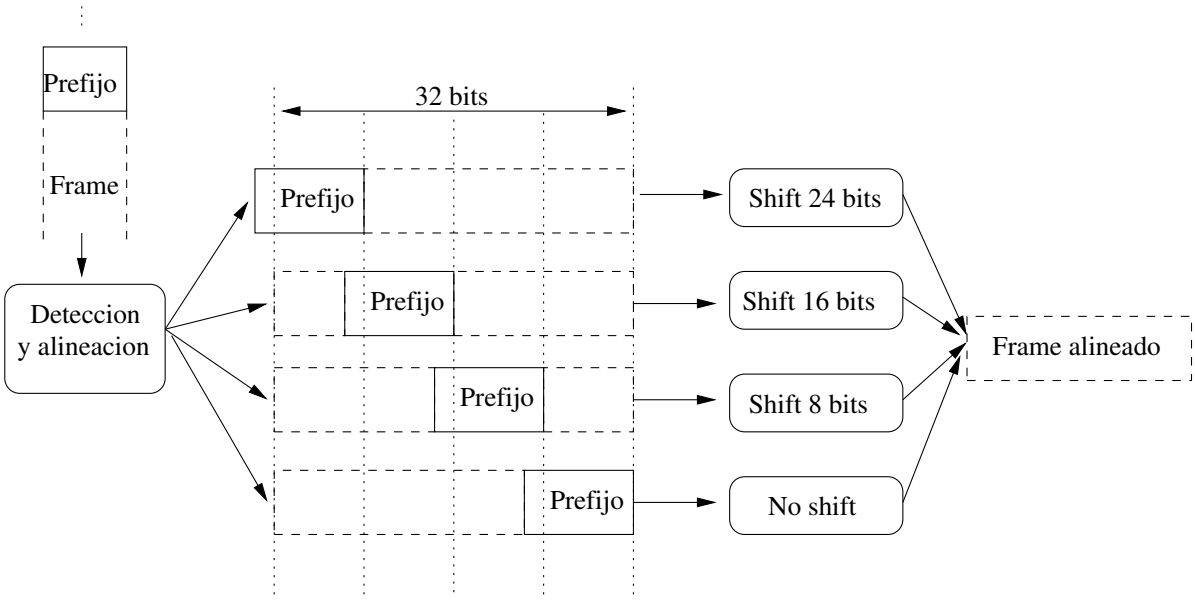



Figura 4.12: Flujo de datos en la sincronización óptica. El mecanismo de sincronización consta de dos etapas: en la primera etapa, el circuito de sincronización de bit alinea la señal entrante al buffer de entrada, colocando el prefijo de sincronización en cuatro posibles alineaciones distintas. La segunda etapa realiza una segunda alineación, detectando la posición del prefijo y utilizando desplazamientos o *shifts* para llevarlo siempre al comienzo del buffer.

1. El cliente que desea establecer un canal seguro envía al principio de sus datos el prefijo de sincronización o *comma* (14 bits). Este prefijo es detectado por el módulo de alineación del receptor, que lo coloca en el buffer de entrada. Sin embargo, no se garantiza que el prefijo este siempre al principio del buffer, sino que puede estar tanto en el bit 0 (que sería una alineación perfecta), como en el bit 8, 16 o 24 (Ver fig.4.12). Esto es debido a que este buffer es de tipo anillo (*ring buffer*).

2. Una vez alineado el prefijo en el buffer de entrada, se detecta en qué posición ha quedado y comenzar a leer la trama desde la posición siguiente. Esto se realiza en el código Verilog sintetizando cuatro detectores que simultáneamente buscan el prefijo en todas las posiciones posibles y deciden en un sólo ciclo de reloj cuál es la alineación correcta. Al haber sólo 4 posiciones, es un algoritmo eficiente.

En teoría, sólo debería realizarse la sincronización al principio de las comunicaciones. En la práctica, los relojes no son perfectos y es necesario sincronizarlos periódicamente. En la implementación óptica, se envía el prefijo de sincronización al comienzo de cada trama. Para evitar colisiones, el hardware de alineamiento se desactiva al detectarse una buena sincronización y se reactiva al finalizar la recepción de la trama. Esta es una operación extremadamente rápida, ya que al utilizar una tasa de 5Gbps, cada trama de 1024 bits tiene una duración temporal de 200 ns. Es necesario aclarar que este prefijo adicional no es parte del protocolo de seguridad diseñado y fue implementado como parte del prototipo. Su utilización en la versión final revelaría información útil a un posible atacante, como por ejemplo el comienzo de la trama.

## 4.4 Redes acústicas

Las señales de audio o acústicas resultaron ser un medio de transmisión compatible con el sistema propuesto. Las señales acústicas se interfieren típicamente de manera aditiva y un modem acústico suele representarse como un canal binario simétrico en lugar de un canal Z. Sin embargo, al utilizar ciertas modulaciones, tales como OOK (*on-off Keying*) en donde la frecuencia portadora es varias veces mayor al ancho de bit, existen bajas posibilidades de que la interferencia de dos señales sea destructiva (es decir, que una señal de audio anule a la otra), mientras que los ceros se modulan como silencios y no causan interferencia. Esto puede aproximarse como un canal Z mediante el cual puede implementarse el sistema de comunicación segura descripto en esta Tesis. Debido a las características de modulación necesarias, las velocidades de transmisión son muy bajas, ya que la respuesta en frecuencia de un transductor acústico típico, como un parlante o micrófono, es relativamente reducida, de 2 KHz a 15 KHz, por lo que el ancho de banda disponible es mucho menor con respecto a la implementación óptica. No obstante, las pruebas e implementaciones sobre este medio pueden ser realizadas totalmente vía software, y el sistema puede ser utilizado en muchas aplicaciones que no requieran elevadas tasas de transmisión

pero que requiera privacidad en la comunicación. Ejemplos de aplicaciones de este tipo pueden ser:

- Aplicaciones bancarias
- Autenticación multi-factor
- Compartir datos de contacto sin necesidad de conexión de red.
- Compartir URLs

La viabilidad de este sistema se demuestra con la reciente publicación de aplicaciones que utilizan este mismo método, utilizando ondas sonoras, para compartir fragmentos de información tales como URLs y contactos. Una aplicación popular de este tipo es Google Tone [96], desarrollada por la empresa Google, que funciona como una extensión de su navegador de Internet.

### 4.4.1 Modulación

Las técnicas de modulación en medios de transmisión acústicos son las mismas que pueden utilizarse en medios electromagnéticos. Sin embargo, no todas las modulaciones siguen el comportamiento de canal Z descripto en la sección 3.3.2. La modulación OOK (un caso especial de modulación ASK, *amplitude shift keying*), es uno de los tipos de modulación que permite implementar un canal Z sobre un medio acústico si se utiliza sobre cierto rango de parámetros. Utilizando transductores (micrófonos y parlantes) comerciales del tipo presentes en la mayoría de los dispositivos móviles, como por ejemplo teléfonos celulares, la frecuencia de portadora puede variar de 10 kHz a 16 kHz. El mejor rendimiento del sistema se obtuvo con una tasa de transmisión de 1 Kbps al nivel de trama. En las secciones siguientes se detallan las mediciones del retraso (*delay*), el tiempo que le lleva a un bit atravesar la red, que es relativamente elevado debido a una combinación de la baja velocidad de transmisión y la necesidad de un buffer relativamente grande (2048 bits), necesario para la utilización del esquema de corrección de errores seleccionado (Reed-Solomon 223/255). Si bien

aumentar la velocidad de transmisión requiere un esfuerzo considerable debido al bajo ancho de banda disponible, la modificación del algoritmo de corrección de errores o sus parámetros (por ejemplo, utilizar algún esquema tipo BCH [61]) podría reducir el retraso de datos de manera considerable.

Para acotar el ancho de banda de la señal emitida, se utilizó la técnica de "*pulse-shaping*", implementada como un filtro FIR [97] (*finite impulse response*) pasa banda a la salida de la etapa de modulación, así como también en la entrada de la etapa de demodulación. Este filtro, además de reducir el ancho de banda utilizado, ayuda a rechazar interferencias. Adicionalmente, un ciclo de trabajo (*duty cycle*) de 50 % demostró ser el óptimo para la modulación.

### 4.4.2 Sincronización

Como se desprende de la descripción del canal de comunicaciones, la sincronización entre el transmisor y el receptor es esencial para la correcta decodificación de la información. En el caso del medio óptico, la sincronización de bit y word (16 bits) debe realizarse a tasas tan elevadas que requiere necesariamente soporte de hardware por parte del transceptor. Sin embargo, las tasas de transmisión de 1 kbps utilizadas en el canal acústico permiten realizar una sincronización por software sin ningún soporte de hardware adicional, al ser una velocidad manejable por cualquier procesador moderno. El método es muy similar al utilizado en el canal óptico: un patrón inicial de sincronización es enviado para que el receptor pueda realizar un ajuste de parámetros tales como fase y umbral de decisión (ver Fig. 4.13). La deriva y fluctuación del reloj del sistema (*drift y jitter*) no son significativas a esta baja velocidad de transmisión, por lo que no se requiere corrección de ningún tipo, haciendo que la implementación del modem por software sea muy sencilla. Ciertos parámetros, si bien son inicializados en la etapa de sincronización, son por naturaleza dinámicos y se ajustan periódicamente, como por ejemplo el umbral de decisión, que es recalculado a partir de un promedio de los datos de entrada. La fase es también corregida utilizando los datos de entrada como referencia. Este método de sincronización permite detectar

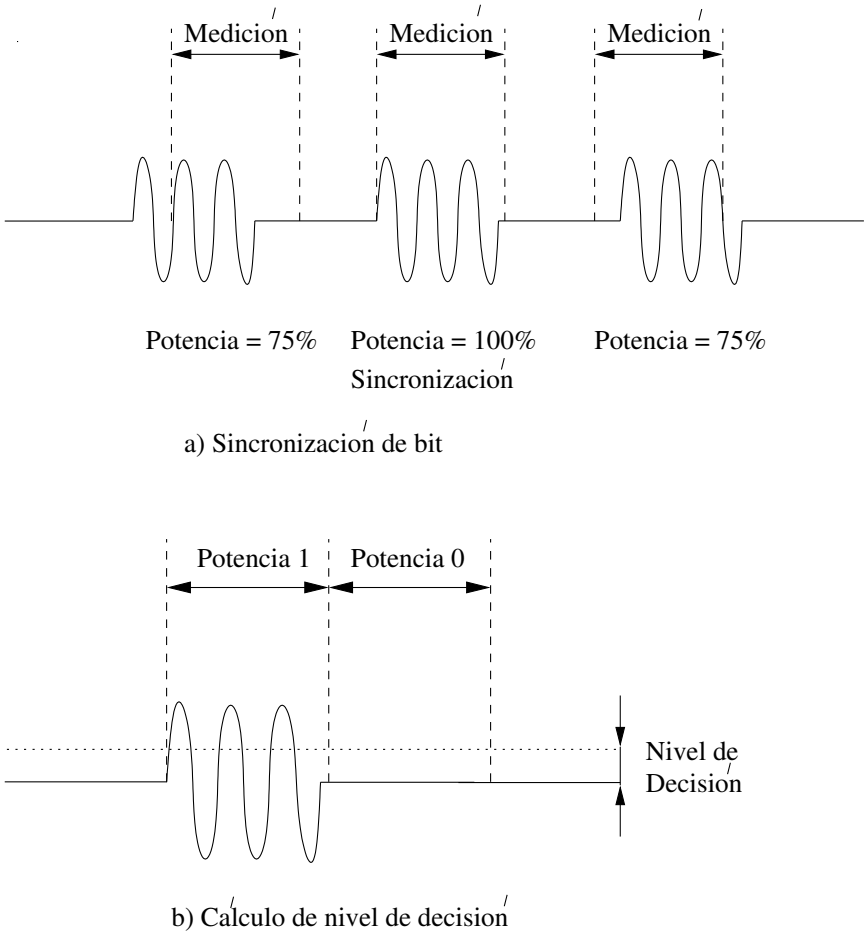



Figura 4.13: Sincronización acústica. En la figura a) se recorren consecutivamente todas las posibilidades hasta encontrar la mayor potencia de bit, que corresponde a la mejor sincronización. Luego, en la figura b) se calcula el umbral de decisión.

el comienzo de la trama a su vez que se ajusta a nivel de bit; ambas alineaciones son necesarias en cada comunicación (pero la alineación de la trama solamente entre los ONUs comunicantes). Adicionalmente, una vez comenzada la transmisión, los datos serán indescifrables gracias al algoritmo CDMA de *time-hopping* guiado por un CS-PRNG.

### 4.4.3 Medición multiusuario

Todas las mediciones fueron realizadas a una tasa de 1 kbps, utilizando una señal portadora acústica de 16 kHz, que se encuentra en el límite auditivo de la mayoría de las

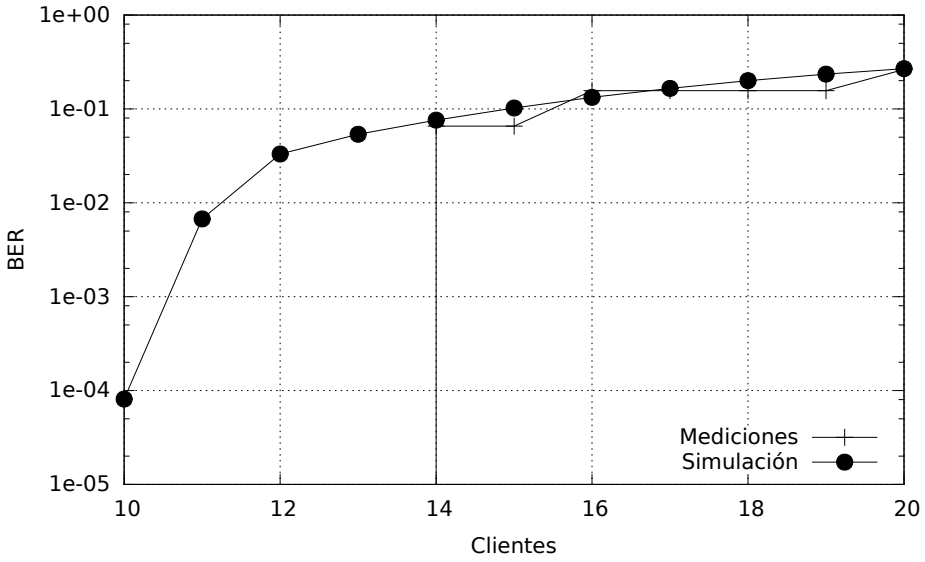



Figura 4.14: Multi-usuario: BER del enlace entre dos laptops (Lenovo T420 y Lenovo X60), una de ellas simulando varios nodos.

personas adultas [98]. Es posible que algunos parlantes no respondan correctamente a esta frecuencia, en cuyo caso puede reducirse y utilizar una portadora de 12 kHz. El objetivo de utilizar una frecuencia de audio tan cercana al límite de reproducción de los transductores es incrementar el nivel de confort de los usuarios, que sólo podrán percibir el modem con bajo volumen, o directamente será inaudible. Adicionalmente, las altas frecuencias presentaron menos interferencias de ruido ambiente. La cantidad total de datos transmitidos por canal fue de 4096 bits en cada medición. El volumen de la señal de salida fue configurado al máximo para cada dispositivo, mientras que la amplificación de la señal obtenida por el micrófono fue optimizada en cada caso para obtener el menor BER. Con el modulador y circuito de sincronización implementados, el sistema opera con tasas de error aceptables con una separación máxima entre nodos de 1 metro, una distancia que normalmente excede la existente entre un terminal móvil (celular, etc.) y una computadora fija en el mismo escritorio (Ver Fig. 4.15). Aún para un alto número de clientes simultáneos ($> 10$) el sistema no presenta altas tasas de error o ancho de banda reducido, como puede verse en la Fig. 4.14. En las mediciones, el retraso del canal fue de más de 60 segundos, excesivo para muchas

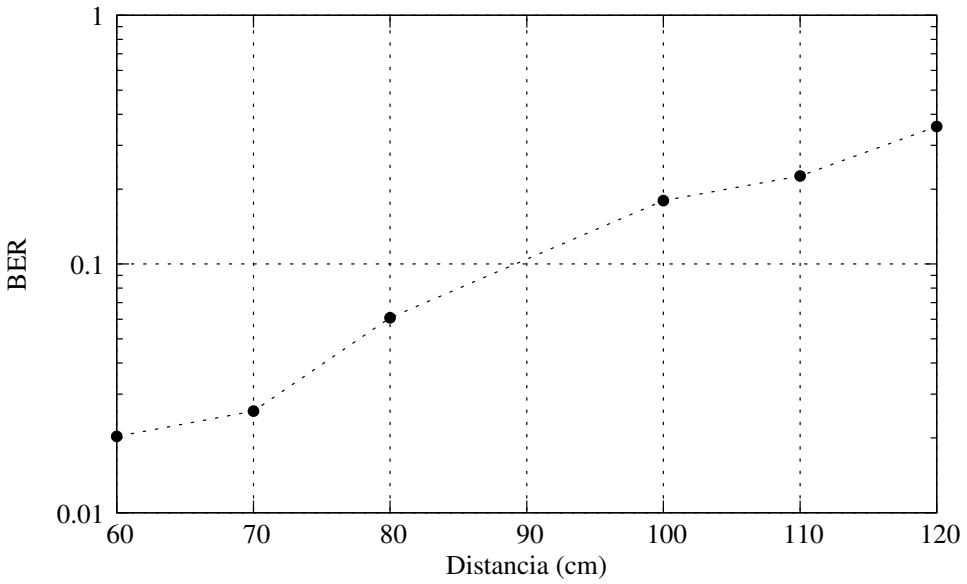



Figura 4.15: Distancia vs. BER: el enlace acústico entre una Laptop (Lenovo T420) y un celular (HTC Status) presenta errores detectables cuando se superan los 60 cm de separación entre ambos dispositivos.

aplicaciones que no necesitan alto ancho de banda pero requieren un corto tiempo de respuesta (por ejemplo, aplicaciones bancarias). El retraso puede ser disminuido de dos maneras:

1. Decrementando la cantidad máxima de clientes simultáneos soportados por el sistema.

2. Utilizando algoritmos de ECC de bajo retraso y de bloque reducido, tales como BCH, ya que actualmente el retraso se produce en su mayor parte durante la recepción de un bloque completo para el algoritmo de Reed-Solomon (2048 bits).

### 4.4.4 Mediciónes a distintas distancias

Las comunicaciones acústicas utilizando como portadora un tono de 12 kHz son muy susceptibles al ruido ambiente. Un enlace acústico con 50 cm de separación entre una notebook Lenovo T420 y un celular HTC Status (ver Fig. 4.15) tuvo un 15 % de BER con sólo una ligera interferencia (como por ejemplo, golpear una mesa cercana). Esta observación motivó el uso de la frecuencia más alta posible. Una portadora de 16

kHz presentó el mayor rango de compatibilidad entre los dispositivos, aunque algunos de ellos demostraron no poder emitir audio a frecuencias mayores. Los parlantes de una Laptop Lenovo T420 y otra Laptop Lenovo X60 fueron capaces de establecer un enlace utilizando como portadora un tono de 19.2 kHz, aunque sólo en cortas distancias (20 cm). De todas formas, esta frecuencia de portadora permitió un mayor ancho de banda en el enlace (2 kbps en lugar de 1 kbps) con la misma tasa de error.

# Capítulo 5

# Conclusiones

En esta Tesis se documentó el diseño un sistema de comunicaciones criptográficamente seguro que aprovecha las técnicas de CDMA sobre fibra óptica y sobre ondas sonoras. Durante el transcurso de la investigación, se desarrolló un algoritmo de corrección de errores asimétrico, optimizado para canales Z.

El resultado es un sistema de red de tipo difusión, capaz de crear múltiples VLANs criptográficamente seguras utilizando cualquier medio de transmisión que pueda ser modelado como un canal Z. Se implementaron simuladores en software con el objetivo de obtener estadísticas y mediciones. Luego se realizaron prototipos funcionales tanto sobre software para el caso del medio acústico, como sobre un dispositivo FPGA en el caso del medio de fibra óptica. El protocolo alcanzó una velocidad de 1000 bps con 16 clientes sobre el medio acústico y 5 Gbps con 128 clientes simultáneos, con una separación máxima de 20 km entre nodos y con una utilización total del medio del 32 %.

Se mostraron resultados de cálculos teóricos, simulaciones numéricas y mediciones realizadas sobre los prototipos.

El esquema de transmisión desarrollado puede utilizarse en cualquier medio de transmisión que pueda representarse como un canal Z, como por ejemplo ondas sonoras o acústicas bajo ciertas modulaciones. Debido a esta característica, el mismo protocolo desarrollado con el objetivo de utilizar fibra óptica como medio de transmisión fue utilizado en una red acústica de baja velocidad entre dispositivos móviles,

con un máximo de 16 dispositivos en la red a una distancia de hasta 1.2 metros. Esto abre las puertas a redes ad hoc privadas entre dispositivos, simplificando aplicaciones que hasta ahora requerían una conexión continua a Internet o de tecnologías del tipo NFC.

Concretamente, se presentó el diseño de una red de difusión con un grado de privacidad criptográficamente fuerte. Para ello se utilizó un filtro de Bloom encriptado, que es utilizado a la vez como el elemento de cifrado y como una primera etapa de corrección de errores. Adicionalmente, se presentó una codificación de datos novedosa que incrementa la eficiencia del filtro de Bloom como algoritmo de corrección de errores. El resultado es un protocolo de VLAN capaz de soportar un volumen de información o *throughput* constante sin importar la carga de la red, manteniendo completa privacidad entre sus nodos.

Se demostró la viabilidad del protocolo mediante la implementación y medición de dos prototipos: el primer prototipo del sistema fue realizado sobre fibra óptica con velocidades de transmisión de 5 Gbps. La plataforma de desarrollo contiene un transceptor láser de comunicaciones del tipo XFP+, y una FPGA del tipo Xilinx Virtex 5. El segundo prototipo fue implementado exclusivamente en software y utiliza el mismo protocolo pero con diferentes parámetros, esta vez sobre una red encriptada acústica entre dispositivos móviles sin ningún tipo de modificación o hardware adicional.

Esta Tesis intenta solucionar uno de los problemas de seguridad más graves de las redes de difusión, que es la vulnerabilidad a ataques de espionaje. Por ejemplo, un nodo malicioso en un sistema TDMA puede acceder a la información de cualquier otro nodo, tan sólo escuchando en el tiempo asignado al nodo víctima, ya que los tiempos de bit son totalmente predecibles.

En contraste, el sistema presentado en esta Tesis asigna los tiempos de bit de manera pseudoaleatoria, por lo que un nodo malicioso no puede predecir la posición de ningún otro nodo. No existe ningún tipo de arbitraje ni de colaboración entre nodos que revela información a un presunto atacante, y se garantiza la comunicación privada de un nodo aún cuando todos los demás nodos del sistema sean maliciosos.

La fuerza criptográfica del sistema está asociada y es equivalente a la del generador pseudoaleatorio seleccionado para generar los tiempos de bit, siendo el único requerimiento del mismo que sea criptográficamente seguro. Al no existir colaboración y arbitraje entre nodos, la naturaleza o algoritmo de dicho generador puede variar de nodo a nodo sin afectar la performance del sistema.

La consecuencia de prohibir toda colaboración o arbitraje es que las colisiones de datos entre nodos son inevitables y frecuentes. El mayor esfuerzo de diseño en el del sistema presentado, y el módulo de mayor consumo de recursos computacionales es la rutina de recuperación o corrección de errores, que debe ser suficientemente potente como para reducir las tasas de error a valores utilizables, sin consumir excesivos recursos computacionales o de ancho de banda. El algoritmo final fue medido con un BER menor a 10e-8 con una utilización del medio del 32 %. Otra característica notable es que, al ser los nodos totalmente independientes entre sí, no se produce ningún tipo de degradación de la velocidad o ancho de banda en los canales de transmisión individuales, siempre y cuando la cantidad total de nodos sea inferior al límite diseñado.

## 5.1 Trabajos futuros

Todos los prototipos realizados son completamente funcionales y cumplen con los objetivos de la Tesis, sin embargo, para una implementación comercial a gran escala es posible optimizar ciertos módulos, que serán nombrados a continuación:

**Codificación** El problema de la codificación de línea fue descrito en 4.3.7 y una solución aceptable, que permite la creación de un prototipo funcional, fue adoptada. Sin embargo, en una implementación final, se debe contemplar la imposibilidad de utilizar cualquier algoritmo de balanceo ya que no es compatible con el algoritmo de filtro de Bloom. Dado que el problema es de naturaleza eléctrica, es probable que un diseño cuidadoso de los buses entre la FPGA y el transceptor óptico solucione este problema.

**Sincronización** El algoritmo de sincronización es crítico en una implementación real. Las implementaciones realizadas para los prototipos son funcionales pero no son ideales ya que, al utilizar prefijos conocidos, un atacante puede obtener información acerca del comienzo y finalización de la trama. La codificación es suficientemente fuerte para que este conocimiento no perjudique el nivel de seguridad, pero es posible el desarrollo de un algoritmo de sincronización criptográficamente seguro, que no revele ninguna información a un posible atacante (en [99] puede verse un ejemplo de sincronización segura).

**Eliminación de la trama** En la sección 2.4 se explica que se divide la transmisión en tramas, que son segmentos de bits cargados directamente dentro del filtro de Bloom. Esta división en segmentos de los datos no es absolutamente necesaria y podría implementarse una variación del algoritmo que no utilice tramas, sino que todas las posiciones de bits sean relativas entre sí, en lugar de relativas al comienzo de la trama. Esta variación no incrementa la seguridad pero, probablemente, simplifique la implementación.

# Bibliografía


[1] Xilinx, "Logicore ip reed-solomon decoder v7.1 data sheet," 2011. [Online] Available: `http://www.xilinx.com/support/documentation/ip_documentation/rs_decoder_ds252.pdf`.

[2] "100g, 200g, 400g: Internet's core is getting fatter to meet our tech planet's bandwidth demand." [Online] Available: `https://gigaom.com/2013/08/16/100g-200g-400g-internets-core-is-getting-fatter-to-meet-our-tech-planets-band`

[3] W. Shieh, H. Bao, and Y. Tang, "Coherent optical ofdm: theory and design," *Optics Express*, vol. 16, no. 2, pp. 841–859, 2008.

[4] W. Kozaczuk, *Enigma: how the German machine cipher was broken, and how it was read by the Allies in World War Two*. Univ Pubns of Amer, 1984.

[5] G. Welchman, *The hut six story: breaking the enigma codes*. McGraw-Hill Companies, 1982.

[6] O. J. Hanas, P. D. Toonder, and F. Pennypacker, "An addressable satellite encryption system for preventing signal piracy," *Consumer Electronics, IEEE Transactions on*, no. 4, pp. 631–636, 1981.

[7] C.-H. Lee, W. V. Sorin, and B. Y. Kim, "Fiber to the home using a pon infrastructure," *Journal of Lightwave Technology*, vol. 24, no. 12, pp. 4568–4583, 2006.

[8] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*. New York, USA: John Wiley & Sons, 2005.

[9] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1st ed., 1996.

[10] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society for Industrial & Applied Mathematics*, vol. 8, no. 2, pp. 300–304, 1960.

[11] B. Li, K. J. Larsen, D. Zibar, and I. T. Monroy, "Forward error correction for 400 gbps high speed optical fiber links," *Forward Error Correcting Codes for 100 Gbit/s Optical Communication Systems*.

[12] R. Gallager and L.-D. P.-C. Codes, "Mit press, 1963," *Low-Density Parity-Check Codes*.

[13] T. Brack, M. Alles, T. Lehnigk-Emden, F. Kienle, N. Wehn, N. E. L'Insalata, F. Rossi, M. Rovini, and L. Fanucci, "Low complexity ldpc code decoders for next generation standards," in *Proceedings of the conference on Design, automation and test in Europe*, pp. 331–336, EDA Consortium, 2007.

[14] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, July, October 1948. [Online] Available: `http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf`.

[15] J. Thorpe, "Low-density parity-check (ldpc) codes constructed from protographs," *IPN progress report*, vol. 42, no. 154, pp. 42–154, 2003.

[16] R. C. Dixon, *Spread spectrum systems: with commercial applications*. John Wiley & Sons, Inc., 1994.

[17] E. Kaplan and C. Hegarty, *Understanding GPS: principles and applications*. Artech house, 2005.

[18] N. Golmie, O. Rebala, and N. Chevrollier, "Bluetooth adaptive frequency hopping and scheduling," in *Military Communications Conference, 2003. MILCOM'03. 2003 IEEE*, vol. 2, pp. 1138–1142, IEEE, 2003.

[19] J. Mikulka and S. Hanus, "Cck and barker coding implementation in ieee 802.11 b standard," in *Radioelektronika, 2007. 17th International Conference*, pp. 1–4, IEEE, 2007.

[20] M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 8, no. 1, pp. 3–30, 1998.

[21] G. Argyros and A. Kiayias, "I forgot your password: Randomness attacks against php applications.," in *USENIX Security Symposium*, pp. 81–96, 2012.

[22] S. K. Park and K. W. Miller, "Random number generators: good ones are hard to find," *Communications of the ACM*, vol. 31, no. 10, pp. 1192–1201, 1988.

[23] D. Coppersmith, H. Krawczyk, and Y. Mansour, "The shrinking generator," in *Advances in Cryptology—Crypto'93*, pp. 22–39, Springer, 1994.

[24] S. Vaudenay and M. Vuagnoux, "Passive–only key recovery attacks on rc4," pp. 344–359, 2007.

[25] R. L. Rivest and J. C. N. Schuldt, "Spritz—a spongy RC4-like stream cipher and hash function." Presented at Charles River Crypto Day (2014-10-24).

[26] N. Firasta, M. Buxton, P. Jinbo, K. Nasri, and S. Kuo, "Intel avx: New frontiers in performance improvements and energy efficiency," *Intel white paper*, 2008.

[27] R. Gold, "Optimal binary sequences for spread spectrum multiplexing (corresp.)," *Information Theory, IEEE Transactions on*, vol. 13, no. 4, pp. 619–621, 1967.

[28] V. IAshchenko, *Cryptography: an introduction*. No. 18, American Mathematical Soc., 2002.

[29] A. Cobham, "The intrinsic computational difficulty of functions," in *Logic, Methodology and Philosophy of Science, proceedings of the second International Congress, held in Jerusalem, 1964* (Y. Bar-Hillel, ed.), (Amsterdam), North-Holland, 1965.

[30] S. S. Greene, *Security policies and procedures*. New Jersey: Pearson Education, 2006.

[31] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is ssl?)," in *Advances in Cryptology—CRYPTO 2001*, pp. 310–331, Springer, 2001.

[32] T. Shake, "Security performance of optical cdma against eavesdropping," *IEEE Journal of Lightwave Technology*, vol. 23, pp. 655–670, Feb. 2005.

[33] W. Meier and O. Staffelbach, "The self-shrinking generator," in *Advances in Cryptology- EUROCRYPT'94* (A. De Santis, ed.), pp. 205–214, Berlin: Springer, 1994.

[34] Algotronix, "Algotronix releases encryption ip cores for otn 400 gbps," 2014. [Online] Available: `http://www.chipestimate.com/news/28314/Algotronix-releases-encryption-IP-cores-for-OTN-`.

[35] Y. J. Jung, C. W. Son, S. Lee, S. Gil, H. S. Kim, and N. Park, "Demonstration of 10 gbps, all-optical encryption and decryption system utilizing soa xor logic gates," *Optical and quantum electronics*, vol. 40, no. 5-6, pp. 425–430, 2008.

[36] J.-m. Liu, H.-F. Chen, and S. Tang, "Synchronized chaotic optical communications at high bit rates," *Quantum Electronics, IEEE Journal of*, vol. 38, no. 9, pp. 1184–1196, 2002.

[37] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, "Experimental open-air quantum key distribution with a single-photon source," *New Journal of physics*, vol. 6, no. 1, p. 92, 2004.

[38] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, (New York), pp. 175–179, IEEE Press, 1984.

[39] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[40] A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *EPL (Europhysics Letters)*, vol. 23, no. 6, p. 383, 1993.

[41] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Physical Review Letters*, vol. 84, no. 20, p. 4729, 2000.

[42] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[43] L. M. Kohnfelder, *Towards a practical public-key cryptosystem.* PhD thesis, Massachusetts Institute of Technology, 1978.

[44] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, pp. 686–689, 2010.

[45] S. Tanakamaru, C. Hung, A. Esumi, M. Ito, K. Li, and K. Takeuchi, "95 %-lower-ber 43 %-lower-power intelligent solid-state drive (ssd) with asymmetric coding and stripe pattern elimination algorithm," in *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2011 IEEE International*, pp. 204–206, IEEE, 2011.

[46] J. M. Berger, "A note on error detection codes for asymmetric channels," *Information and Control*, vol. 4, no. 1, pp. 68–73, 1961.

[47] I. Neri, N. Skantzos, and D. Bollé, "Gallager error-correcting codes for binary asymmetric channels," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2008, no. 10, p. P10018, 2008.

[48] G. Kramer and G. Pesavento, "Ethernet passive optical network (epon): building a next-generation optical access network," *Communications magazine, IEEE*, vol. 40, no. 2, pp. 66–73, 2002.

[49] P. Chanclou, B. Capelle, B. Charbonnier, J. Courant, Y. Denis, N. Genay, S. Gosselin, D. Kurz, B. Landousies, E. Le Bris, *et al.*, "France telecom's pon deployment, learnt lessons and next steps," in *Optical Fiber Communication Conference, Proc. OFC/NFOEC*, 2013.

[50] armoredshield, "Armored spon," Aug. 2012. [Online] Available: `http://www.armoredshield.com/armored-spon.html`.

[51] G. Cincotti, N. Wada, and K.-i. Kitayama, "Secure ocdm-based pon," in *Optical Fiber Communication Conference*, p. OThI6, Optical Society of America, 2009.

[52] N. Nadarajah, E. Wong, and A. Nirmalathas, "Implementation of multiple secure virtual private networks over passive optical networks using electronic cdma," *Photonics Technology Letters, IEEE*, vol. 18, no. 3, pp. 484–486, 2006.

[53] D. G. Steer, L. Strawczynski, W. Diffie, and M. Wiener, "A secure audio teleconference system," in *Proceedings on Advances in cryptology*, pp. 520–528, Springer-Verlag New York, Inc., 1990.

[54] Arcelect, "Aes encrypted modem," Aug. 2014. [Online] Available: `http://www.arcelect.com/Encrypted_AES_Modem.htm`.

[55] S. H. Kellert, *In the wake of chaos: Unpredictable order in dynamical systems*. University of Chicago press, 1994.

[56] R. Gnanajeyaraman, K. Prasadh, *et al.*, "Audio encryption using higher dimensional chaotic map," 2009.

[57] P. Gallagher and C. Kerry, "Fips pub 186-4: Digital signature standard, dss (2013)."

[58] G. D. Forney and G. D. Forney, *Concatenated codes*, vol. 11. Citeseer, 1966.

[59] T. Richardson, "Error floors of ldpc codes," in *Proceedings of the annual Allerton conference on communication control and computing*, vol. 41, pp. 1426–1435, The University; 1998, 2003.

[60] S. B. Wicker and V. K. Bhargava, *Reed-Solomon codes and their applications*. John Wiley & Sons, 1999.

[61] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Information and control*, vol. 3, no. 1, pp. 68–79, 1960.

[62] P. Karn, "Biblioteca de algoritmos de corrección de errores," Aug. 2007. [Online] Available: `http://www.ka9q.net/code/fec/`.

[63] Xilinx, "Logicore ip reed-solomon encoder v7.1 data sheet," Mar. 2011. [Online] Available: `http://www.xilinx.com/support/documentation/ip_documentation/rs_encoder_ds251.pdf`.

[64] T. J. McCabe, "A complexity measure," *Software Engineering, IEEE Transactions on*, no. 4, pp. 308–320, 1976.

[65] T. C. Coding, "Consultative committee for space data systems," tech. rep., CCSDS 101.0-B-4, May, 1999.

[66] D. J. C. MacKay, *Information Theory, Inference & Learning Algorithms*. New York, NY, USA: Cambridge University Press, 2002.

[67] L. G. Tallini, S. Al-Bassam, and B. Bose, "On the capacity and codes for the z-channel," in *Proc. IEEE International Symposium on Information Theory (ISIT'02)*, (Lausanne, Switzerland), p. 422, June 2002.

[68] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Commun. ACM*, vol. 13, pp. 422–426, July 1970.

[69] H. Song, S. Dharmapurikar, J. Turner, and J. Lockwood, "Fast hash table lookup using extended bloom filter: an aid to network processing," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4, pp. 181–192, 2005.

[70] N. Nadarajah, E. Wong, and a. Nirmalathas, "Implementation of multiple secure virtual private networks over passive optical networks using electronic CDMA," *IEEE Photonics Technology Letters*, vol. 18, pp. 484–486, Feb. 2006.

[71] S. S. Gupta, A. Chattopadhyay, K. Sinha, S. Maitra, and B. P. Sinha, "High-performance hardware implementation for rc4 stream cipher," *IEEE Transactions on Computers*, vol. 62, no. 4, pp. 730–743, 2013. [Online] Available: `http://doi.ieeecomputersociety.org/10.1109/TC.2012.19`.

[72] D. E. Thomas and P. R. Moorby, *The Verilog® Hardware Description Language*, vol. 2. Springer Science & Business Media, 2002.

[73] P. Sepehrdad, S. Vaudenay, and M. Vuagnoux, "Statistical attack on rc4 distinguishing wpa," in *Proceedings of the 30th Annual International Conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT'11, (Berlin, Heidelberg), pp. 343–363, Springer-Verlag, 2011. [Online] Available: `http://dl.acm.org/citation.cfm?id=2008684.2008712`.

[74] D. Eastlake and J. Schiller, "S. crocker,randomness requirements for security," tech. rep., BCP 106, RFC 4086, June, 2005.

[75] O. Solutions, "Transceiver sfp / duplex." [Online] Available: `http://www.oesolution.com/products/communication/`.

[76] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *Journal of Communications*, vol. 8, pp. 758–767, Nov. 2013. [Online] Available: `http://www.jocm.us/index.php?m=content&#38;c=index&#38;a=show&#38;catid=124&#38;id=600`.

[77] K. August, T. Sizer, and G. Wright, "Apparatus and method for initiating a transaction having acoustic data receiver that filters human voice," June 11 2002. [Online] Available: `http://www.google.com/patents/CA2232316C?cl=en`.

[78] A. Ortega, V. Bettachini, J. Alvarez-Hamelin, and D. Grosz, "Hamming-weight minimisation coding for cdma optical access networks with enhanced security," in *Future Generation Communication Technology (FGCT), 2012 International Conference on*, pp. 185–189, Dec 2012.

[79] P. V. Nikitin, K. Rao, and S. Lazar, "An overview of near field uhf rfid," in *IEEE international Conference on RFID*, vol. 167, Citeseer, 2007.

[80] G. P. Agrawal, *Fiber-Optic Communication Systems*. New York, USA: John Wiley & Sons, second ed., 1997.

[81] X. Virtex, "Fpga ml507 evaluation platform," 5.

[82] X. U. Virtex, "Fpga rocket i/o gtp transceiver user guide," 5. [Online] Available:ttp://www.xilinx.com/virtex5.

[83] Xilinx, "Ml507 four gtxs ibert quickstart," 2006. [Online] Available: http://www.xilinx.com/products/boards/ml507/ml507_10.1_1/docs/ml507_ibert_4gtxs_quickstart.pdf.

[84] K. Arshak, E. Jafer, and C. Ibala, "Testing fpga based digital system using xilinx chipscope logic analyzer," in *Electronics Technology, 2006. ISSE'06. 29th International Spring Seminar on*, pp. 355–360, IEEE, 2006.

[85] Xilinx, "Ug198 virtex-5 fpga rocketio gtx transceiver user guide," 2006. [Online] Available: http://www.xilinx.com/support/documentation/user_guides/ug198.pdf.

[86] Altera, "Transceiver altera." [Online] Available: https://www.altera.com/solutions/technology/transceiver/overview.html.

[87] A. Serial, "High-speed serialized at attachment," *Serial ATA working group, available at www.sata-io.org*, 2001.

[88] R. Budruk, D. Anderson, and T. Shanley, *PCI express system architecture*. Addison-Wesley Professional, 2004.

[89] A. X. Widmer and P. A. Franaszek, "A dc-balanced, partitioned-block, 8b/10b transmission code," *IBM Journal of research and development*, vol. 27, no. 5, pp. 440–451, 1983.

[90] Xilinx, "Logicore ip microblaze micro controller system," 2012. [Online] Available: http://www.xilinx.com/support/documentation/sw_manuals/xilinx13_4/ds865_microblaze_mcs.pdf.

[91] S. Committee *et al.*, "Sff-8431 specifications for enhanced small form factor pluggable module sfp+," *Appendix D, Revision*, vol. 4.

[92] X. Virtex, "Xilinx inc. platform cable usb ii." [Online] Available: http://www.xilinx.com/products/boards-and-kits/HW-USB-II-G.htm.

[93] Xilinx, "Ug347 ml505/ml506/ml507 evaluation platform, user guide," 2006. [Online] Available: http://www.xilinx.com/support/documentation/user_guides/ug347.pdf.

[94] Xilinx, "Ug366 virtex-6 fpga gtx transceiver," 2009. [Online] Available: http://www.xilinx.com/support/documentation/user_guides/u366.pdf.

[95] A. Ortega, V. A. Bettachini, D. F. Grosz, and J. I. Alvarez-Hamelin, "Altas velocidades de transferencia en fibra óptica utilizando FPGAs de bajo costo," in *Congreso de Microelectrócnica Aplicada 2010* (D. Brenji, ed.), (San Justo), pp. 126–129, Universidad Nacional de la Matanza (UNLaM), 2010.

[96] "Google tone: An experimental chrome extension for instant sharing over audio." [Online] Available: http://googleresearch.blogspot.com.ar/2015/05/tone-experimental-chrome-extension-for.html.

[97] A. V. Oppenheim, R. W. Schafer, J. R. Buck, *et al.*, *Discrete-time signal processing*, vol. 2. Prentice-hall Englewood Cliffs, 1989.

[98] S. Gordon-Salant, "Hearing loss and aging: new research findings and clinical implications," *Journal of rehabilitation research and development*, vol. 42, no. 4, p. 9, 2005.

[99] O. Jung and C. Ruland, "Encryption with statistical self-synchronization in synchronous broadband networks," in *Cryptographic Hardware and Embedded Systems*, pp. 340–352, Springer, 1999.