Optimización aplicada al sistema de intercambio de clave segura KLJN con garantía de error máximo fijo

Optimization applied to the KLJN secure key exchange system with maximum fixed error guarantee

Edwin Collado[1], Yessica Sáez[2]*
[1]Centro de Innovación y Transferencia Tecnológica, Universidad Tecnológica de Panamá, [2] Centro Regional de Azuero, Universidad Tecnológica de Panamá
[1]edwin.collado@utp.ac.pa, [2]yessica.saez@utp.ac.pa

Resumen– *El sistema de intercambio de clave segura KLJN ha demostrado proveer seguridad incondicional de forma simple y con muy pocos componentes electrónicos. Sin embargo, este sistema presenta errores estadísticos que dependen de parámetros como la ventana de tiempo para realizar el intercambio de la clave y otros que son relevantes en la interpretación de los bits de la clave. El objetivo de este trabajo es desarrollar estrategias que permitan obtener valores óptimos de dichos parámetros, mientras se asegura que los errores se mantengan dentro de valores aceptables. Los resultados obtenidos demuestran que las técnicas de optimización propuestas no solo garantizan que los errores no sobrepasen un límite de error máximo fijo permitido, sino que también permiten manejar eficientemente los recursos del sistema al utilizar valores óptimos de los parámetros importantes en el análisis de error.*

Palabras claves–*Optimización, probabilidad de error, ruido de Johnson, seguridad incondicional, sistema KLJN.*

Abstract– *The KLJN secure key exchange system has been proven to provide unconditional security in a simple way with very few electronic components. However, this system presents statistical errors that depend on parameters such as the time window for performing the key exchange and other relevant parameters used in the interpretation of the key bits. The objective of this work is to develop strategies to obtain optimal values of these parameters while ensuring that errors are kept within acceptable values. The results show that the proposed optimization techniques not only guarantee that the errors do not exceed a fixed maximum allowed error limit, but also allows to efficiently manage the system resources by using optimal values of the important parameters in the error analysis.*

Keywords–*Optimization, error probability, Johnson´s noise, unconditional security, KLJN system.*

Tipo de Artículo: Original
Fecha de Recepción: 24 de febrero de 2017
Fecha de Aceptación: 25 de septiembre de 2017

1. Introducción

La comunicación electrónica se ha convertido en una de las partes más importantes de las actividades cotidianas del ser humano. Una gran cantidad de información, en su mayoría confidencial y sensible, es enviada, recibida y/o almacenada cada segundo. Por tal razón, resulta esencial contar con medidas de seguridad adecuadas que garanticen las cuatro características básicas de seguridad en una red de telecomunicaciones: autenticación, integridad, confidencialidad y no repudio [1]. Autenticación para garantizar la identidad de los que se comunican en la red, integridad para asegurar que usuarios no autorizados no puedan leer y/o modificar la información que se transmite, confidencialidad para asegurar que la comunicación permanezca privada y protegida todo el tiempo, y no repudio para que los involucrados en el proceso de comunicación no puedan negar haber enviado/recibido un mensaje [1], [2]. Existen numerosos métodos y algoritmos orientados a asegurar estas características [2], donde uno de las más importantes es el cifrado o criptografía de datos [3].

El cifrado consiste en aplicar un algoritmo con cierta clave para transformar los mensajes y así garantizar la

confidencialidad [3]. Existen dos técnicas principales de cifrado, una de ellas es el cifrado asimétrico, el cual utiliza dos claves, una públicamente conocida y una privada, para cifrar y descifrar información, respectivamente. La otra técnica, y el foco de atención en el contexto de este trabajo, es el cifrado simétrico, en donde las dos partes involucradas en la comunicación (a menudo llamados *Alice* y *Bob*), generan e intercambian una sola clave, usualmente representada por una secuencia aleatoria de dígitos binarios (*bits*), para cifrar y descifrar la información.

Durante el proceso de intercambio de la clave simétrica, existe la posibilidad de que un usuario no autorizado (un espía, a menudo denominado *Eve*) esté monitorizando continuamente la comunicación. Por lo tanto, la seguridad en la comunicación depende grandemente de la capacidad que tengan *Alice* y *Bob* para intercambiar la clave de seguridad de forma secreta, mientras *Eve* monitoriza/escucha dicho intercambio.

Lastimosamente, la mayoría de los métodos empleados para generar e intercambiar esta clave, son basados en software y solo proveen un nivel de seguridad (computacionalmente) condicional. A simple vista, dichos métodos parecen inquebrantables, sin embargo, su efectividad no está totalmente garantizada en el futuro [4]-[7], ya que con acceso a un poder de computación adecuado o a un algoritmo lo suficientemente eficiente, un espía podría descubrir la clave y obtener acceso a la información que haya sido cifrada con la misma.

En contraste al cifrado digital, se encuentran los esquemas de intercambio de clave de capa física, los cuales son técnicas alternativas para ocultar información de espías. Dichas soluciones prometen ser incondicionalmente seguras [1]. Esto quiere decir que, a nivel teórico, la información se mantiene segura, incluso cuando *Eve* cuente con un poder de computación infinito y velocidad y precisión de medición ilimitadas. Es importante mencionar que la implementación práctica de dichos sistemas, en los cuales la clave tiene una longitud finita y se cuenta con un tiempo limitado para realizar el intercambio, puede no mantener esa seguridad incondicional. Sin embargo, desde el punto de vista probabilístico, el objetivo es lograr que el espía tenga una probabilidad muy pequeña de romper la seguridad [4], [5].

El primer esquema de seguridad en clamar seguridad incondicional fue el sistema de distribución de clave cuántica (QKD, *quantum key distribution*) [8]. Sin embargo, existen debates entre expertos sobre los niveles de seguridad alcanzados en este sistema [9]-[13]. Además, aunque discusiones indican que a través de nuevos enfoques (Ver [14], [15]) se podrían lograr niveles de seguridad más satisfactorios, todavía existen ciertas limitaciones prácticas como su precio, tamaño, cobertura, entre otros.

Afortunadamente, un prometedor sistema físico-clásico, de bajo costo, fue propuesto como alternativa para proveer seguridad incondicional utilizando solamente unos cuantos resistores, interruptores y cables [16]. Este sistema, conocido como *intercambio de clave segura KLJN* (*Kirchhoof´s-Law-Johnson-Noise*), está basado en las leyes de circuito de Kirchhoff y el teorema de fluctuación-disipación de física estadística. Su seguridad contra ataques pasivos (aquellos ataques en los que el espía trata de obtener información sin modificar la misma ni los recursos del sistema [1]) se basa en última instancia en la segunda ley de termodinámica [6], [16]-[20].

La simplicidad y el rendimiento del sistema KLJN han sido confirmados a través de su demostración experimental [17], cuyos resultados han motivado propuestas de modificaciones al sistema para mejorar su velocidad, cobertura y seguridad [21]-[25]. También se han propuesto una gran cantidad de aplicaciones potenciales, incluyendo distribución de clave segura en redes eléctricas inteligentes (*Smart Grids*) [26] y en comunicaciones vehiculares [26], [27] e informáticas [28], así como protección en componentes de hardware, procesadores, dispositivos de almacenamiento masivo, entre otras [29].

Como toda realización práctica, el sistema KLJN presenta limitaciones debido a su comportamiento en presencia de no-idealidades (tolerancia de las resistencias, capacitancia, resistencia e inductancia en el cable, efectos transitorios, entre otras [4], [6], [16]-[18]). Es por esto que se han propuesto y se siguen proponiendo (como en todo esquema físico de intercambio de clave) diversos tipos de ataques. Afortunadamente, hasta el momento, para los ataques propuestos existen mecanismos de defensa que han demostrado ser efectivos [21], [22].

El principio de funcionamiento del sistema KLJN se basa en mediciones de la media cuadrática del ruido (voltaje y/o corriente) del canal entre *Alice* y *Bob*. Dado que los mismos, cuentan con una ventana de tiempo finita para realizar dichas mediciones en el canal, los resultados de las mismas pueden presentar inexactitudes estadísticas. En consecuencia, se presentan errores en la interpretación de los valores de *bit* en el sistema [30]-[32].

Las probabilidades de los diferentes tipos de error en el sistema KLJN fueron estimadas en [30]-[32]. Se observó que dicha probabilidad de errores de *bits* depende grandemente de ciertos parámetros del sistema, presentados en secciones posteriores. Por ello, con el objetivo de reducir la probabilidad de que estos errores de mediciones ocurran, este trabajo busca desarrollar estrategias de seguridad, basadas en optimización, para encontrar valores óptimos de dichos parámetros que garanticen que la probabilidad de error de bit no sobrepase un límite máximo permitido. Los resultados muestran que al utilizar técnicas de optimización se puede asegurar que los errores se mantengan dentro de un valor aceptable, mientras se asegura una fidelidad razonable en el sistema.

El resto de este artículo está organizado de la siguiente manera. La sección 2 describe el modelo conceptual del sistema de intercambio de clave segura KLJN. La sección 3 presenta la formulación de los problemas de optimización para encontrar los valores óptimos de los parámetros relevantes en el análisis de error. La sección 4 ilustra, a través de simulaciones, la funcionalidad y beneficios de optimizar el sistema de seguridad propuesto. Finalmente, la sección 5 presenta un resumen de los resultados; junto con importantes iniciativas de investigación que se considerarán en el futuro.

2. Sistema de intercambio de clave segura KLJN

A continuación se presenta una descripción del principio de funcionamiento ideal del sistema de intercambio de clave segura KLJN y un resumen del análisis de errores en este esquema.

2.1 Descripción del sistema KLJN

La figura 1 muestra el circuito esquemático del sistema KLJN [4], [6], [16], [17], [21], [22]. Este circuito no presenta elementos de defensa contra ataques activos (o invasivos, es decir ataques en los que el usuario malicioso modifica intencionalmente el sistema con el objetivo de extraer información [1]), ni contra ataques dirigidos a vulnerabilidades representadas por elementos de construcción no ideales.

El canal de comunicación KLJN es un cable. Ambas partes involucradas en la comunicación, *Alice* y *Bob*, cuentan con un par idéntico de resistores, R_0 y R_1, en donde $R_0 \neq R_1$ y generalmente $R_1 >> R_0$. Estos resistores se utilizan para indicar los dígitos binarios de la clave, donde R_0 representa el valor de bit 0 mientras que R_1 representa el valor de bit 1. Los generadores de voltaje ruido Gaussiano $u_{0,A}(t)$, $u_{1,A}(t)$ y $u_{0,B}(t)$, $u_{1,B}(t)$ representan ya sea el ruido de Johnson de los resistores R_0 y R_1 de *Alice* y *Bob*, respectivamente; o generadores externos de ruido blanco con un ancho de banda público, denotado como B_{KLJN} y temperatura efectiva T_{eff} [4], [6], [16], [17], [21], [22].

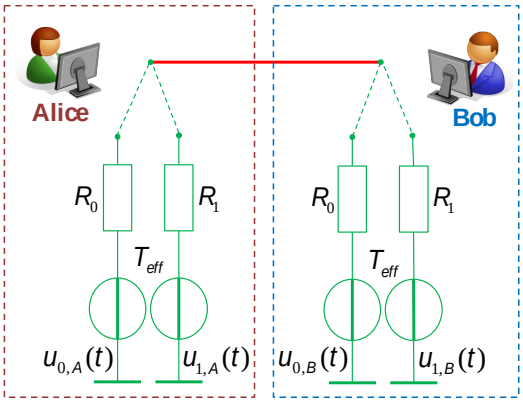

Figura 1. Circuito esquemático del sistema KLJN [4], [6], [16], [17], [21], [22].

Al inicio de cada período de reloj, también denominado período de intercambio de bit, *Alice* y *Bob*, quienes están sincronizados en el tiempo, seleccionan aleatoriamente uno de los dos resistores y lo conectan al cable. La configuración del sistema una vez se seleccionen los resistores se muestra en figura 2. Por lo tanto, existen cuatro posibles situaciones de *bits* en las que estos dos pares de resistores pueden conectarse a la línea de cable: 00, 01, 10 y 11.

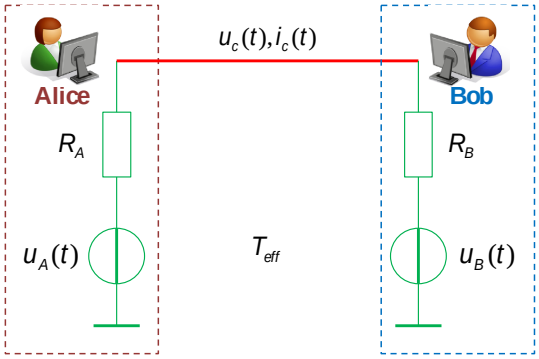

Figura 2. Circuito esquemático del sistema KLJN luego de que *Alice* y *Bob* conectan el resistor seleccionado aleatoriamente [4], [6], [16], [17], [21], [22].

De acuerdo con el teorema de fluctuación-disipación, el voltaje de ruido de Johnson de los resistores de *Alice* y *Bob*, denotados $u_A(t)$ y $u_B(t)$, donde $u_A(t) \in \{u_{0,A}(t),\ u_{1,A}(t)\}$ y $u_B(t) \in \{u_{0,B}(t),\ u_{1,B}(t)\}$, generan un voltaje de ruido de canal $u_c(t)$ entre el cable y tierra, y una corriente de ruido en el cable, denotada $i_c(t)$.

Dentro del período de intercambio de bit, *Alice* y *Bob* (y también *Eve*), miden la media cuadrática de las amplitudes de voltaje y/o corriente de ruido, es decir $\langle u_c^2(t) \rangle$ y/o $\langle i_c^2(t) \rangle$. Aplicando la fórmula de Johnson y las leyes de circuito de Kirchhoff, se tiene que los valores teóricos de las medias cuadráticas de las amplitudes de voltaje y corriente de ruido, para un ancho de banda de ruido de canal B_{KLJN} y una temperatura T_{eff}, son [4] [16]:

$$\langle u_c^2(t) \rangle = 4kT_{eff} R_{\|} B_{KLJN} \qquad (1)$$

y

$$\langle i_c^2(t) \rangle = 4kT_{eff} \frac{1}{R_{loop}} B_{KLJN}, \qquad (2)$$

respectivamente [4], [16]. En donde $\langle u_c^2(t) \rangle$ y $\langle i_c^2(t) \rangle$ representan los promedios de tiempo infinito (ideal) del cuadrado del voltaje y corriente de ruido del canal, respectivamente, k es la constante de Boltzman y $R_{\|}$ y R_{loop} representan la conexión en paralelo y serie de los resistores seleccionadas aleatoriamente por *Alice* y *Bob*, es decir, $R_{\|} = \frac{R_A R_B}{R_A + R_B}$ y $R_{loop} = \frac{1}{R_A + R_B}$, para $R_A, R_B \in \{R_0, R_1\}$.

Es importante mencionar que los valores de $R_{\|}$ y R_{loop} pueden ser conocidos públicamente al medir la media cuadrática del voltaje y/o corriente de ruido del canal y compararlos con los valores teóricos de ecuaciones (1) y (2) [16]. Debido a que tanto *Alice* como *Bob* conocen cuáles de sus resistores han sido conectados al canal, las resistencias $R_{\|}$ y R_{loop} les permite deducir el valor de la resistencia (y por ende el valor de bit) al otro lado del cable [16].

Aquellos casos en que tanto *Alice* como *Bob* seleccionan los mismos resistores, es decir los casos de bit 00 y 11, representan un intercambio inseguro de bit. Esto es porque en estos casos *Eve* sería capaz de deducir los valores de los resistores y su ubicación y por ende el valor del bit, debido a que $R_{\|}$ y/o R_{loop} sería el máximo o mínimo de sus tres posibles valores de magnitud. En contraste, los casos cuando ambas partes seleccionan aleatoriamente resistores diferentes, es decir, las situaciones de bit 10 y 01, son considerados como eventos de intercambio seguro de bit porque de acuerdo con la segunda ley de termodinámica [6], [16]-[20], las mediciones de las medias cuadráticas no les permiten a *Eve* determinar los valores y ubicaciones de los resistores.

Es importante notar que al final de un intercambio seguro de bit, *Alice* y *Bob* terminan con valores de *bits* opuestos. Debido a que en los sistemas de cifrado simétrico ambas partes deben tener la misma clave, *Alice* y *Bob* deben acordar previamente (antes de iniciar el intercambio) quién de los dos invertirá su bit, para así contar con la misma secuencia de *bits* en ambos lados. Además, en promedio, el 50% de los *bits* se mantiene porque son seguros y el otro 50% son descartados por el sistema por ser inseguros [16].

La siguiente sección presenta el análisis de error de *bits* presentado en [30]-[32] y sus respectivas expresiones matemáticas.

2.2 Errores de dígitos binarios en el sistema KLJN

El principio de funcionamiento del sistema KLJN se basa en mediciones de media cuadrática del ruido (voltaje y/o corriente) del canal. Alice y Bob (y también Eve) cuentan con una ventana de tiempo finita para realizar dichas mediciones. Esta ventana, conocida como el período de intercambio de bit, es denotada como $\tau = \frac{1}{f_B}$, donde $f_B << B_{KLJN}$, es la frecuencia de

intercambio de bit. Debido a esto, los resultados de las mediciones de las amplitudes de ruido de canal presentan inexactitudes estadísticas, ya que si el tiempo disponible para Alice y Bob no es lo suficientemente grande como para obtener estadísticas suficientemente buenas, los mismos no pueden distinguir entre los diferentes niveles de magnitud de la media cuadrática de ruido del canal. En consecuencia, se presentan errores en la interpretación de los valores de bit en el sistema [30]. Dichos errores pueden llegar a ser significativos, especialmente cuando se utilizan algoritmos de amplificación de privacidad (PA, privacy amplification) [25], ya que estos tienden a amplificar los errores.

El proceso de medición de la media cuadrática del ruido del canal y la interpretación de *bits* ha sido minuciosamente descrito en la literatura [47]-[49]. Por simplicidad, se procederá a mostrar el proceso para estimar los errores de dígitos binarios cuando el sistema solo mide el voltaje ruido del canal. Un procedimiento similar se puede seguir para el caso de mediciones de corriente.

La figura 3 ilustra los tres posibles niveles de la media cuadrática del voltaje de ruido del canal para las situaciones 00, 01/10 y 11.

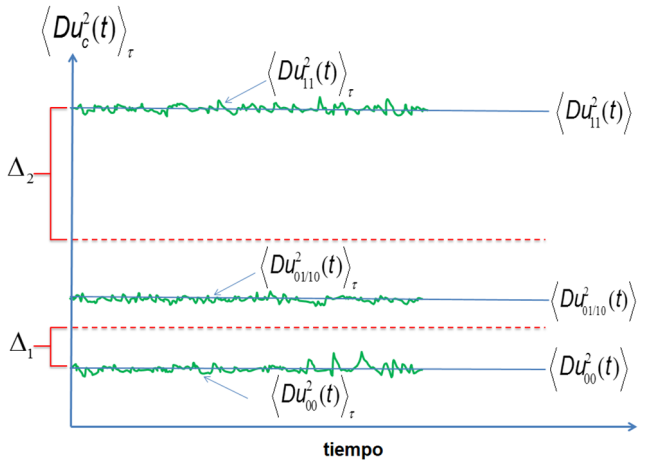

Figura 3. Posibles niveles de la media cuadrática del voltaje de ruido del canal (escala arbitraria).

Los valores $\langle Du_{11}^2(t)\rangle_\tau$, $\langle Du_{10/01}^2(t)\rangle_\tau$ y $\langle Du_{11}^2(t)\rangle_\tau$ representan las medias cuadráticas para las situaciones 11, 10/01 y 00, respectivamente. Las líneas sólidas representan las mediciones cuando se cuenta con un tiempo infinito (ideal). Por simplificad, $R_0 = \alpha R_1$ para $\alpha >> 1$. Figura modificada de la versión original, traducida al español [30].

Cabe resaltar que la medición final de la media cuadrática del voltaje de ruido del canal está dada por: $\langle Du_c^2(t)\rangle_\tau = \langle Du_c^2(t)\rangle + \mu_\tau(t)$, donde $\langle Du_c^2(t)\rangle \in \{\langle Du_{11}^2(t)\rangle, \langle Du_{10/01}^2(t)\rangle, \langle Du_{00}^2(t)\rangle\}$ representa la componente DC, es decir, los valores exactos (ideales) de las medias cuadráticas cuando se cuenta con una ventana de tiempo medición τ infinita, $D = \frac{1}{1\,\text{Voltio}}$ es el coeficiente de transferencia del dispositivo multiplicador hipotético para proporcionar una unidad de Voltio también para el cuadrado del valor del voltaje de ruido [33], y $\mu_\tau(t)$ representa la componente AC generada al obtener el valor medio en un tiempo finito y que está ilustrada por las fluctuaciones (aleatorias) alrededor del valor DC (Ver figura 3).

Con muy poca probabilidad, las fluctuaciones (Gaussianas con alta precisión [33]) de los valores promedio medidos, podrían cruzar de un nivel a otro y producir una interpretación de bit errónea por parte de *Alice* y *Bob*, causando así un error de bit. Por tal motivo, en [30] se definieron valores umbrales Δ_1 y Δ_2 (Ver figura 3) para determinar los límites entre los diferentes niveles para la interpretación de las magnitudes de la media cuadrática de voltaje de ruido de canal durante el tiempo τ. Dichos umbrales fueron definidos, para fines de normalización, como una fracción de la componente DC de la media cuadrática del voltaje de ruido de canal medido, es decir [30]:

$$\Delta_1 = \beta\langle Du_{00}^2(t)\rangle \text{ para } 0 < \beta < 1 \quad (3)$$

y

$$\Delta_2 = \delta\langle Du_{11}^2(t)\rangle \text{ para } 0 < \delta < 1. \quad (4)$$

Las interpretaciones de las mediciones de las medias cuadráticas del voltaje de ruido del canal son: [30]

- 00, para $\langle Du_c^2(t)\rangle_\tau < \langle Du_{00}^2(t)\rangle + \Delta_1$,
- 11, para $\langle Du_c^2(t)\rangle_\tau > \langle Du_{11}^2(t)\rangle - \Delta_2$, y
- 10/01, para $\langle Du_{00}^2(t)\rangle + \Delta_1 \le \langle Du_c^2(t)\rangle_\tau \le \langle Du_{11}^2(t)\rangle - \Delta_2$.

La tabla 1 resume los diferentes tipos de errores de interpretación de mediciones que podrían ocurrir en el sistema KLJN debido a imprecisiones estadísticas [30].

De acuerdo la tabla 1, los errores en los que la decisión final del sistema es una situación de *bit* no

segura (00 y 11) son autocorregidos por el sistema, ya que el mismo descarta todas las situaciones que comprometen información acerca de la clave. Por lo tanto, solo los casos cuando las situaciones de bit actuales 00 y 11 son interpretados erróneamente como la situación de bit segura 01/10, son de interés [30].

Para estimar las probabilidades de los diferentes tipos de error en el sistema KLJN, en [30] se utilizó la fórmula de Rice [34], [35], la cual calcula el número promedio de cruces por un nivel fijo por un proceso estocástico en un intervalo de tiempo.

Las fórmulas analíticas de las probabilidades de error en el sistema KLJN cuando se mide voltaje de ruido del canal, fueron estimadas con la probabilidad de que las componentes AC, $\mu_\tau(t)$, crucen los umbrales especificados para cada tipo de error, durante el tiempo τ. La estimación de la probabilidad de error se basa en el hecho de que, en el límite de error pequeño, la probabilidad de tener repetidos cruces de umbral dentro del tiempo de correlación del ruido de banda limitada converge a cero. Además, como el tiempo de correlación de $\mu_\tau(t)$ es igual a τ, cada cruce de umbral (en una dirección fija elegida)

Tabla 1. Tipos de errores en el sistema KLJN [30]*(Traducida al español)

		Situación Actual		
		00	11	01/10
Interpretación de la Medición	00	Correcto (sin error)	Error, removido (automáticamente)	Error, removido (automáticamente)
	11	Error, removido (automáticamente)	Correcto (sin error)	Error, removido (automáticamente)
	01/10	Error (probabilidad?)	Error (probabilidad?)	Correcto (sin error)

indica un error independiente. Por lo tanto, una buena estimación de las probabilidades de error en este límite de error, es el producto del promedio de la frecuencia de cruces de los umbrales Δ_1 y Δ_2, y el tiempo τ [36], [37].

Las probabilidades $\varepsilon_{u,00}$ y $\varepsilon_{u,11}$, que denotan los errores cuando las situaciones 00 y 11 se interpretan como la situación 01/10, en el modo de medición de voltaje de ruido, para $\varepsilon_{u,00}, \varepsilon_{u,11} << 1$, están dados por, respectivamente [30]:

$$\varepsilon_{u,00} \approx \frac{1}{\sqrt{3}} \exp\left(-\frac{\beta^2}{4} \gamma \right) \qquad (5)$$

y

$$\varepsilon_{u,11} \approx \frac{1}{\sqrt{3}} \exp\left(-\frac{\delta^2}{4} \gamma \right), \qquad (6)$$

donde $\gamma = \frac{B_{KLJN}}{f_B} = B_{KLJN} \tau$.

A pesar de que estas fórmulas capturan la influencia de los valores de umbral en los errores de *bit*, la única información que conocemos sobre estos valores de umbral es que fueron definidos como una fracción de la componente DC de la media cuadrática del voltaje de ruido del canal. Por lo tanto, uno de los objetivos de este artículo es desarrollar una estrategia basada en optimización para encontrar los valores de umbral óptimos para la interpretación de los *bits* de la clave en el sistema KLJN, mientras se limita la probabilidad de error de bit permitida.

Además, las expresiones de probabilidad de error muestran una dependencia exponencial de la duración del periodo de intercambio de *bits* (es decir, la ventana de tiempo disponible para realizar estadística), como se muestra en las ecuaciones (5) - (6). Es decir, cuanto más tiempo *Alice* y *Bob* tienen que hacer estadísticas, mayor es la fidelidad del sistema KLJN. Desafortunadamente, aumentar el período de intercambio de bits también significa aumentar la tasa de conjetura de bits exitosa de *Eve*. Esto se debe a que, para situaciones prácticas, los ataques pasivos exitosos de *Eve* están restringidos por la duración del período de intercambio de *bits*. Por lo tanto, en este trabajo también se propone un enfoque basado en técnicas de optimización para encontrar el valor óptimo de la ventana de tiempo de medición que garantiza la probabilidad de error de *bit* para una fidelidad fija del sistema KLJN y un ancho de banda de ruido fijo. De esta manera, se asegura no solo una fidelidad del sistema razonablemente buena, sino que también debilitará las estadísticas de *Eve* al restringir la duración del período de intercambio de *bits*.

3. Formulación del problema

En esta sección, se describe la formulación de los problemas para la optimización de los valores de umbral y de la ventana de tiempo de medición para garantizar que la probabilidad de error de *bit* permanezca dentro de cierto límite aceptable. Por simplicidad, el análisis se hará para la probabilidad de error $\varepsilon_{u,00}$, es decir para los errores cuando la situación 00 se interpreta como la situación 01/10 en el modo de medición de voltaje de ruido. Sin embargo, una formulación similar se puede realizar para la probabilidad $\varepsilon_{u,11}$ y también para los errores en el modo de medición de corriente de ruido.

3.1 Optimización de los valores de umbral para interpretación de los *bits* de la clave en el sistema KLJN

La idea es obtener el valor de umbral óptimo que garantice que la probabilidad de error de *bit* permanezca por debajo del valor máximo de error permitido. Este valor óptimo de umbral, puede ser visto como el valor mínimo necesitado de β para el diseño de un sistema KLJN que asegure cierto valor de probabilidad de error de bit. La solución de este problema está dada por $\beta_{\inf} \le \beta < 1$, en donde $\beta_{\inf}$ representa el valor óptimo de umbral.

El problema de optimizar los valores de umbral para maximizar el error de probabilidad está formulado como:

$$\max_{\beta} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2 \gamma}{4} \right) \tag{7}$$

sujeto a

$$\frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2 \gamma}{4} \right) \le \varepsilon_{\sup} \tag{7.1}$$

$$0 < \beta < 1 \ , \tag{7.2}$$

donde $\varepsilon_{\sup}$ representa el valor máximo de error permitido por el diseñador del sistema de antemano, (7.1) garantiza que la probabilidad de error no sobrepase el nivel máximo estipulado y (7.2) define el rango para los valores de umbral.

El problema (7) puede ser fácilmente resuelto utilizando distintas herramientas de optimización [38].

3.2 Optimización del valor de la ventana de tiempo de medición que garantiza la probabilidad mínima de error de *bit*

El objetivo es desarrollar una estrategia de seguridad basada en optimización que obtenga el valor óptimo de ventana de tiempo de medición τ para asegurar que la probabilidad de error de *bits* permanezca dentro del límite deseado para un sistema KLJN con fidelidad fija y ancho de banda de ruido fijo. De esta forma, no solo se asegura una fidelidad aceptable del sistema, sino que también se debilita las estadísticas de Eve al restringir la duración del período de intercambio de *bits*.

Este valor óptimo de τ puede ser visto como el valor mínimo requerido para garantizar cierto nivel de probabilidad de error de *bit* en el sistema. La solución de este problema está dada por $\tau_{\inf} \le \tau \le 50\tau_{BKLJN}$, en donde $\tau_{\inf}$ representa el valor óptimo de τ.

$$\min_{\tau} = \frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2 B_{KLJN} \tau}{4} \right) \tag{9}$$

sujeto a

$$\frac{1}{\sqrt{3}} \exp\left(\frac{-\beta^2 B_{KLJN} \tau}{4} \right) \le \varepsilon_{\sup} \ , \tag{9.1}$$

$$0 < \tau \le 50\tau_{BKLJN} \ , \tag{9.2}$$

donde la definición de γ fue utilizada, específicamente $\gamma = \frac{B_{KJLJN}}{f_B} = B_{KLJN}\tau$, $\varepsilon_{\sup}$ representa el valor máximo de error permitido por el diseñador del sistema, τ_{BKLJN} representa el tiempo de correlación del ruido, definido como $\tau_{BKLJN} \approx \frac{1}{B_{KLJN}}$, y el límite superior de τ fue elegido en base a las demostraciones experimentales presentadas en [5], en donde estadísticas de ruido de alta fidelidad fueron alcanzados cuando $\tau = 50\tau_{BKLJN}$. También, (7.1) garantiza que la probabilidad de error no sobrepase el nivel máximo estipulado y (7.2) define el rango para τ.

Observe que el problema (9) también puede ser resulto facialmente utilizando herramientas de optimización similares.

4. Resultado Numéricos y Simulaciones

A continuación, se presentan los resultados numéricos y simulaciones para los problemas de optimización de los valores de umbral utilizados en la interpretación de *bits* y la ventana de tiempo de medición para garantizar que la probabilidad de error de bit permanezca dentro de cierto valor aceptable.

4.1 Optimización de los valores de umbral para la interpretación de los *bits* de la clave en el sistema KLJN

Para este caso, se consideró el siguiente escenario: $\varepsilon_{\sup} = 0.025$, $0 < \beta < 0.7$, $B_{KLJN} = 1000\,Hz$, $\gamma = [50\ 100\ 150\ 200\ 250]$, en donde el rango de los valores de β fue calculado para valores concretos de R_0 y R_1, específicamente $R_0 = 2kOhm$ y $R_1 = 11kOhm$, tal como se utilizaron en [5]. Esto es porque por razones obvias (el sistema se quedaría sin *bits* seguros), β no puede aproximarse a 1.

En tabla 2 se muestran los valores óptimos obtenidos del umbral $\beta_{\inf}$ cuando el valor de γ varía. Estos resultados fueron obtenidos utilizando la fórmula para el valor óptimo del umbral $\beta_{\inf}$ en (8). Esto también puede ser observado en la figura 4.

Nótese que este problema obtiene el valor mínimo de $\beta_{\inf}$ (representado con "*" en figura 4) que garantiza $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de γ.

Tabla 2. Valores óptimos de $\beta_{\inf}$ que garantizan $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de γ

γ	$\beta_{\inf}$
50	0.2241
100	0.2506
150	0.2893
200	0.3544
250	0.5012

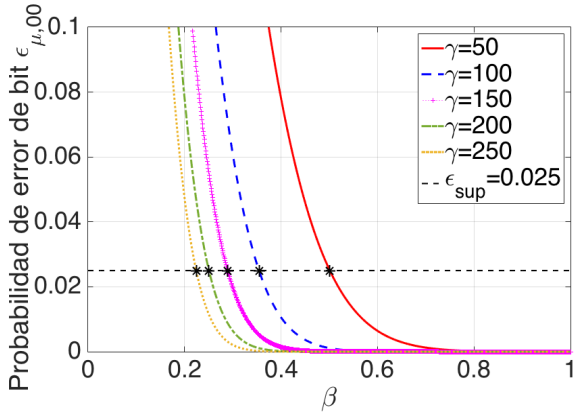

Figura 4. Valores mínimos de β que garantizan $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de γ.

Además, se puede observar que los valores de β dependen grandemente del valor de probabilidad de error $\varepsilon_{u,00}$ deseado. La figura 5 muestra los valores de β necesarios para garantizar cierto valor de $\varepsilon_{u,00}$ cuando $\tau = \frac{50}{B_{KLJN}}$. Se puede observar que los valores de $\varepsilon_{u,00}$ incrementan a medida que los valores de β decrecen, lo cual es esperado ya que se necesita un valor alto de β para obtener un valor bajo de $\varepsilon_{u,00}$. También, se observa que esta estrategia de seguridad garantiza una probabilidad de error de bit no mayor a 0.57 bajo ciertas asunciones.

Este resultado puede ser de gran importancia al momento de diseñar estrategias de seguridad para garantizar cierto nivel de error en escenarios complejos.

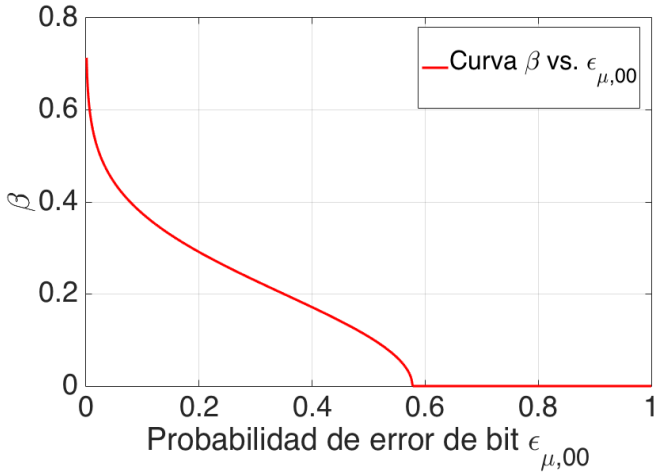

Figura 5. Valores de β necesarios para garantizar cierto valor de $\varepsilon_{u,00}$ cuando $\tau = \frac{50}{B_{KLJN}}$.

4.2 Optimización del valor óptimo de la ventana de tiempo de medición que garantiza la probabilidad mínima de error de *bit*

Para este caso, se consideró el siguiente escenario: $\varepsilon_{\sup} = 0.025$, $0 < \tau < \frac{50}{B_{KLJN}}$, $B_{KLJN} = 1000\,Hz$, $\beta = [0.50\ 0.55\ 0.60\ 0.65\ 0.70]$. Para este escenario, cualquier valor de β menor a 0.50 provee siempre una probabilidad de error de bit mayor a $\varepsilon_{\sup}$ para todos los valores de τ.

Tabla 3 muestra los valores óptimos obtenidos del periodo de intercambio de *bits* $\tau_{\inf}$ cuando el valor de β varía. Estos resultados fueron obtenidos utilizando la

fórmula para el valor óptimo del período de intercambio de *bits* $\tau_{\inf}$ en (10).

Tabla 3. Valores óptimos de $\tau_{\inf}$ que garantizan $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de β.

β	$\tau_{\inf}$ (s)
0.50	0.0500
0.55	0.0413
0.60	0.0347
0.65	0.0296
0.70	0.0255

Los resultados mostrados en tabla 3 y figura 6, demuestran el beneficio de diseñar e implementar estrategias de optimización que obtienen el valor mínimo de $\tau_{\inf}$ (representado con "*" en figura 6) que garantiza $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de β. Este modelo, además de garantizar un nivel de probabilidad de error deseado, también permite manejar eficientemente los recursos del sistema al utilizar el valor óptimo del periodo de intercambio de *bits*, el cual es inversamente proporcional a la tasa de muestreo utilizado.

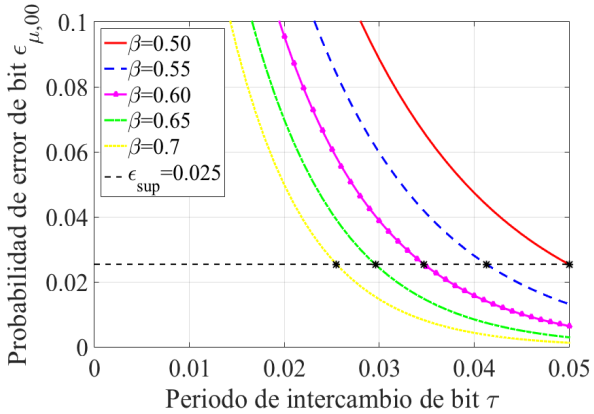

Figura 6. Valores óptimos de $\tau_{\inf}$ que garantizan $\varepsilon_{u,00} \le \varepsilon_{\sup}$ para diferentes valores de β.

Es imprescindible mencionar que la seguridad en sistemas de comunicación cableada utilizando el intercambio de clave segura KLJN es un tema considerablemente nuevo, el cual solo ha sido estudiado matemáticamente y empíricamente en laboratorios [16]-[20]. El presente trabajo utiliza los resultados específicos del análisis de errores en el sistema KLJN presentado en [31]-[32], y se aplica optimización a ese modelo específico. Lamentablemente, al ser la primera vez que se le aplican técnicas de optimización a este modelo de análisis de error para este sistema, no es posible encontrar otros resultados para evaluar y comparar. Sin embargo, el plan a futuro es utilizar otros modelos de optimización con el fin de mejorar el rendimiento del propuesto en este artículo.

5. Conclusiones

En este estudio se presentó un nuevo enfoque para optimizar el sistema de intercambio de clave segura KLJN, con el fin de garantizar que la probabilidad de error de *bits* permanezca siempre dentro del límite permitido. La estrategia de optimización propuesta se enfoca principalmente en controlar óptimamente el umbral para la interpretación de los *bits* de la clave y la ventana de tiempo para realizar el intercambio de dichos *bits*, ya que se ha demostrado que los errores estadísticos dependen principalmente de estos parámetros. Además de esto, el problema de optimización consta de restricciones que permiten garantizar que la probabilidad de error de *bits* no podrá sobrepasar el valor deseado establecido de antemano por el diseñador.

Los resultados numéricos mostraron que las estrategias de optimización propuestas para optimizar el sistema de intercambio de clave segura KLJN, no sólo garantizan que los errores no sobrepasen el límite de error máximo fijo permitido, sino que también permite manejar eficientemente los recursos del sistema al utilizar valores óptimos de los parámetros importantes en el análisis de error. Adicionalmente, se puede concluir que estas estrategias no solo aseguran una fidelidad del sistema razonablemente buena, sino que también debilitan las estadísticas de *Eve* al restringir la duración del período de intercambio de *bits*.

Este trabajo se enfoca principalmente en analizar la probabilidad de error entre *Alice* y *Bob* y no considera la probabilidad de error de *Eve*. En este sentido, estrategias para optimizar el sistema de intercambio de clave segura KLJN que garanticen también que la probabilidad de error de *Eve* siempre permanezca por encima de un valor deseado podría considerarse una extensión importante de este estudio.

6. Contribución de los Autores

Los autores declaran haber contribuido por igual en la escritura, simulación y análisis de datos de este artículo.

7. Referencias

[1] Y. Liang, H. V. Poor, and S. Shamai. "Information Theoretic Security." Foundations and Trends in Communications and Information Theory 5, pp.355–580, Jun. 2008.

[2] W. Ford. *Computer Communications Security: Principles, Standard Protocols and Techniques*. Prentice-Hall, Inc, 1994.

[3] D. Stinson. *Cryptography: Theory and Practice*. CRC press, 2005.

[4] R. Mingesz, L.B. Kish, Z. Gingl, C.G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera. "Unconditional Security by the Laws of Classical Physics." Metrology and Measurement Systems 20.1, pp.3–16, Mar. 2013.

[5] R. Mingesz, L. B. Kish, Z. Gingl, C.G. Granqvist, H. Wen, F. Peper, T. Eubanks, and G. Schmera. "Information Theoretic Security by the Laws of Classical Physics." Soft Computing Applications: Proeedings of the 5th International Workshop Soft Computing Applications (SOFA), Springer Berlin-Heidelberg, pp. 11–25, 2013.

[6] L. B. Kish, D. Abbott, and C. G. Granqvist. "Critical Analysis of the Bennett-Riedel Attack on Secure Cryptographic Key Distributions via the Kirchhoff-Law-Johnson-Noise Scheme." *PLoS ONE* 8.12, e81810, Dec. 2013.

[7] E. Gonzalez, L. B. Kish, and R. S. Balog. "Information Theoretically Secure, Enhanced Johnson Noise based Key Distribution over the Smart Grid with Switched Filters." *PLoS ONE* 8**,** e70206, 2013.

[8] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. "Quantum Cryptography, or Unforgeable Subway Tokens." *Advances in Cryptology:* Advances in Cryptology, Plenum Press, pp. 267–275, 1982.

[9] H. P. Yuen. "On the Foundations of Quantum Key Distribution- Reply to Renner and Beyond." Manuscript: arXiv:1210.2804, Oct. 2012.

[10] H. P. Yuen. "Unconditional Security in Quantum Key Distributions." Manuscript: arXiv:1205.5065v2, May 2012.

[11] O. Hirota. "Incompleteness and Limit of Quantum Key Distribution Theory." Manuscript: arXiv:1208.2106v2, Aug. 2012.

[12] R. Renner. "Reply to Recent Scepticism about the Foundations of Quantum Cryptography." Manuscript: arXiv:1209.2423v.1, Sept. 2012.

[13] H. P. Yuen. "Security Significance of the Trace Distance Criterion in Quantum Key Distribution." Manuscript: arXiv:1109.2675v3, Sept. 2012.

[14] H. P. Yuen. "Key Generation: Foundation and a New Quantum Approach." IEEE Journal Selected Topics in Quantum Electronics 15 pp.1630–1645, Nov. 2009.

[15] H. Salih, Z. H. Li, M. Al-Amri, and H. Zubairy. "Protocol for Direct Counterfactual Quantum Communication." Physical review letters 110.17 p.170502, Apr. 2013.

[16] L. B. Kish. "Totally Secure Classical Communication Utilizing Johnson (-like) Noise and Kirchhoff's Law." Physics Letters A 352.3, pp.178–182, Mar. 2006.

[17] R. Mingesz, Z. Gingl, and L. B. Kish. "Johnson (-like)-Noise-Kirchhoff-Loop Based Secure Classical Communicator Characteristics, for Ranges of Two to Two Thousand Kilometers, Via Model-Line." Physics Letters A 372.7, pp.978–984, Feb. 2008.

[18] L. B. Kish and T. Horvath. "Notes on Recent Approaches Concerning the Kirchhoff-Law-Johnson-Noise-Based Secure Key Exchange." Physics Letters A 373.32, pp.901–904, Aug. 2009.

[19] L. B. Kish and C. G. Granqvist. "On the Security of the Kirchhoff-Law-Johnson-Noise (KLJN) Communicator." Quantum Information Processing 13.10, pp.2213-2219, Oct. 2014.

[20] D. Abbott and G. Schmera. "Secure Communications Using the KLJN Scheme." Scholarpedia 8.8, p.31157, Aug. 2013.

[21] L. B. Kish. "Protection Against the Man in the Middle attack for the Kirchhoff-Loop Johnson(-like)-Noise Cipher and Expansion by Voltage-Based Security." Fluctuation and Noise Letters 6.01, pp.L57-L63, Mar. 2005.

[22] L. B. Kish. "Enhanced Secure Key Exchange Systems Based on the Johnson-Noise Scheme." Metrology and Measurement Systems 20.2 pp. 191-204, Jun. 2013.

[23] L. B. Kish and C. G. Granqvist. "On the Security of the Kirchhoff-Law-Johnson-Noise (KLJN) Communicator." Quantum Information Processing, 13.10, pp.2213-2219, Oct. 2014.

[24] L. B. Kish. "Enhanced Usage of Keys Obtained by Physical, Unconditionally Secure Distributions." Manuscript: http://arxiv.org/abs/1408.5800, 2014.

[25] T. Horvath, L.B. Kish, and J. Scheuer. "Effective Privacy Amplification for Secure Classical Communications." Europhysics Letters (EPL) 94.2, p.28002, Apr. 2011.

[26] Y. Saez, X. Cao, L. B. Kish, and G. Pesti. "Securing Vehicle Communication Systems by the KLJN Key Exchange Protocol." Fluctuation and Noise Letters 13, p.1450020, Sep. 2014.

[27] X. Cao, Y. Saez, L. B. Kish, and G. Pesti. "On KLJN-Based Secure Key Distribution in Vehicular Communication Networks." Fluctuation and Noise Letters 14, p.1550008, Mar. 2015.

[28] L. B. Kish and R. Mingesz. "Totally Secure Classical Networks with Multipoint Telecloning (Teleportation) of Classical *Bits* Through Loops with Johnson-Like Noise." Fluctuation and Noise Letters 6.02, pp.C9–C21, Jun. 2006.

[29] L. B. Kish and O. Saidi. "Unconditionally Secure Computers, Algorithms and Hardware, such as Memories, Processors, Keyboards, Flash and Hard Drives." Fluctuation and Noise Letters 8.02, pp.L95-L98, Jun. 2008.

[30] Y. Saez and L. B. Kish. "Errors and their Mitigation at the Kirchhoff-Law-Johnson-Noise Secure Key Exchange." PLoS ONE 8.11, p.e81103, Nov. 2013.

[31] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist. "Current and Voltage Based Bit Errors and their Combined Mitigation for the Kirchhoff-Law–Johnson-Noise Secure Key Exchange." Journal of Computational Electronics 13.1, pp.271-277, Mar. 2014.

[32] Y. Saez, L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist. "Bit Errors in the Kirchhoff-Law-Johnson-Noise Secure Key Exchange." International Journal of Modern Physics Conference Series 33, p.1460367, 2014.

[33] L. B. Kish, R. Mingesz, Z. Gingl, and C. G. Granqvist. "Spectra for the Product of Gaussian Noises." Metrology and Measurement Systems, 19(4), pp.653-658, 2012.

[34] S. O. Rice. "Mathematical Analysis of Random Noise." Bell Labs Technical Journal 23.3, pp.282-332, 1944.

[35] I. Rychlik. "On Some Reliability Applications of Rice's Formula for the Intensity of Level Crossings." Extremes 3.4, pp.331-348, Dec. 2000.

[36] L. B. Kish. “End of Moore's Law; Thermal (Noise) Death of Integration in Micro and Nano Electronics.” Physics Letters A 305.3, pp.144–149, Dec. 2002.
[37] L. B. Kish and C. G. Granqvist. “Electrical Maxwell Demon and Szilard Engine Utilizing Johnson Noise, Measurement, Logic and Control.” PLoS ONE 7, p.e46800, 2012.
[38] S. Boyd and L. Vandenberghe. Convex optimization. Cambridge Univ. Press, Cambridge, UK: Cambridge University.