Universitat Oberta de Catalunya

uoc.edu

Simulador de comunicación satelital con sistema QKD

Irene López Solier

Máster Universitario en Ingeniería de Telecomunicación
Sistemas de Comunicación

Tutor/a de TF
Javier Jordán Parra
Profesor/a responsable de la asignatura
Carlos Monzo Sánchez

12/06/2023

Universitat Oberta de Catalunya

Ficha del Trabajo Final

Título del trabajo:	Simulador de comunicación satelital con sistema QKD
Nombre del autor/a:	Irene López Solier
Nombre del Tutor/a de TF:	Javier Jordán Parra
Nombre del/de la PRA:	Carlos Monzo Sánchez
Fecha de entrega:	12/06/2023
Titulación o programa:	Máster Universitario en Ingeniería de Telecomunicación
Área del Trabajo Final:	Sistemas de Comunicación
Idioma del trabajo:	Castellano
Palabras clave	Comunicación cuántica, Sistema *QKD*, Satélite

Resumen del Trabajo

La comunicación cuántica se encuentra actualmente en auge debido a su potencial para conseguir mayor seguridad en las comunicaciones y con ello complementar los sistemas actuales de telecomunicación para toda aplicación que así lo requiera. Dicha seguridad se consigue con la distribución de claves cuánticas, *Quantum Key Distribution* (*QKD*), la cual permite que los datos cifrados que se envíen puedan descifrarse mediante claves que han sido codificadas y transmitidas en un estado cuántico.

Uno de los escenarios en el que se prevé la aplicación de la comunicación cuántica es en las comunicaciones satelitales, y por este motivo el propósito del presente trabajo es desarrollar un simulador capaz de analizar las prestaciones de la comunicación en un escenario básico, estableciendo el enlace de comunicación en espacio libre entre una estación terrena y un satélite. El objetivo es que dicho simulador pueda ser utilizado en el ámbito educacional para el estudio y análisis de este tipo de comunicaciones.

Para el desarrollo del simulador se ha considerado necesario introducir primero el marco teórico ligado a la comunicación satelital tradicional (canal de comunicación clásico) y a los sistemas *QKD* (canal cuántico). Luego se ha presentado el desarrollo del simulador, realizado con MATLAB, que permite configurar diferentes parámetros del escenario para simular cómo sería la comunicación en cada caso.

Por último, se presentan los resultados obtenidos tras la simulación de ciertas configuraciones del escenario, analizando y comparando resultados.
Así, el simulador desarrollado permite analizar las prestaciones del enlace de comunicación bajo determinadas configuraciones del escenario.

Abstract

Quantum communication is currently booming due to its potential to achieve greater security in communications and thus complement current telecommunication systems for any application that requires it. That security is achieved using Quantum Key Distribution (QKD), which allows the encrypted data that is sent to be decrypted by keys that have been encoded and transmitted in a quantum state.
A scenario in which the application of quantum communication is foreseen is in satellite communications, and for this reason the purpose of this work is to develop a simulator capable of analyzing the performance of communication in a basic scenario, establishing the link communication in free space between an earth station and a satellite. The objective is this simulator can be used in the educational field for the study and analysis of this type of communications.
For the simulator development, it has been considered necessary to first introduce the theoretical framework linked to traditional satellite communication (classical communication channel) and QKD systems (quantum channel). Then, the simulator has been presented, developed using MATLAB, which allows configuring different parameters of the scenario to simulate how the communication would be in each case.
Finally, the obtained results after simulating certain scenario configurations are presented, analyzing and comparing results.
Thus, the developed simulator allows analyzing the performance of the communication link under certain scenario configurations.

Índice

Lista de Figuras

1. Introducción

1.1. Contexto y justificación del Trabajo

Conforme avanza la evolución tecnológica, son cada vez más las teorías que consiguen implementarse de forma práctica, primero con grandes esfuerzos y a nivel de investigación, y más adelante encontrando la forma de realizar implementaciones eficientes capaces de cubrir necesidades que ya existían o incluso otras nuevas que van surgiendo a la par que la propia evolución de la tecnología.

La distribución de claves cuánticas (*QKD*) es una de las tecnologías cuánticas con más madurez, y que promete mejorar mucho el nivel de seguridad de las comunicaciones. Al permitir un intercambio seguro de claves gracias a la aplicación de las leyes de la mecánica cuántica, se presenta como un seguro ante los retos y amenazas que presenta la computación cuántica de romper los actuales sistemas de intercambio de claves.

Por otra parte, la comunicación cuántica presenta actualmente limitaciones importantes en cuanto a la distancia que puede cubrirse en enlaces terrestres mediante el uso de fibra óptica debido a las pérdidas que esta presenta y a que aún no existen equipos desplegables capaces de actuar como repetidores cuánticos de la señal, pues los que existen aún están en fase de laboratorio. Esto hace que el segmento espacial, mediante el uso de satélites, brinde una oportunidad para poder establecer enlaces a mayores distancias de las conseguidas actualmente en el segmento terrestre.

En el caso de la comunicación cuántica, una de sus aplicaciones más relevantes es precisamente la distribución de claves cuánticas para conseguir que la información transmitida, que puede ser interceptada por terceros, sea más segura y fiable.
Uno de los escenarios de aplicación para este tipo de comunicaciones es el satelital, que actualmente se utiliza a nivel mundial principalmente para cubrir aquellas áreas donde no es posible realizar un despliegue de infraestructuras terrestres. Aunque actualmente el escenario más utilizado en comunicaciones clásicas es el enlace entre una estación terrena y un satélite para así establecer comunicación entre dos estaciones terrenas mediante el satélite, también hay que considerar ya las aplicaciones que requieren de establecer una comunicación cuántica intersatelital (*Inter-Satellite Link, ISL*).

El enlace entre estación terrena y satélite, en espacio libre, presenta una serie de características que pueden afectar tanto al canal de comunicación clásico (basado en el uso de señales de radiofrecuencia) como al canal de comunicación cuántico (basado en el uso de señales ópticas). Ya existen hoy en día muchas herramientas para realizar balances de enlace en comunicación satelital sobre el canal clásico en radiofrecuencia, pero aún no hay un avance tecnológico lo suficientemente maduro como para una aplicación masiva de la

comunicación cuántica, y por tanto en el caso del canal cuántico no existen herramientas de este tipo fácilmente accesibles.
Por dicho motivo, el objetivo del trabajo es desarrollar un simulador que permita analizar cuáles serían las prestaciones del enlace de comunicación descrito si este se quiere usar para la distribución de claves cuánticas (*QKD*), de manera que sea de ayuda en el ámbito educacional para el estudio y análisis de este tema sobre un escenario simplificado pero lo suficientemente representativo para su entendimiento. Para el análisis será necesario por tanto que el simulador devuelva una serie de resultados (principalmente gráficos) que permitan al usuario evaluar las prestaciones del enlace y su uso con sistemas *QKD*.

1.2. Objetivos del Trabajo

A continuación se detallan los diferentes objetivos del presente trabajo:

- Definir el marco teórico necesario para establecer las bases a aplicar sobre el canal clásico y el canal cuántico en espacio libre, considerando un escenario de comunicación entre una estación terrena y un satélite.

- Diseñar y desarrollar un simulador para comunicaciones satelitales con sistema *QKD*, mediante MATLAB, que permita analizar las prestaciones básicas del canal de comunicación.

- Explicar el funcionamiento del simulador a modo de manual de usuario para que sea fácilmente entendible por la comunidad educativa, a la que está dirigido su uso.

- Analizar los resultados obtenidos para diferentes configuraciones del escenario establecido, comparando dichos resultados para establecer las conclusiones obtenidas.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

En términos de sostenibilidad, el presente trabajo no tiene impactos negativos en cuanto al medio ambiente y/o huella ecológica, pero sí puede considerarse cierto impacto positivo sobre el ODS 9 – *Industry, innovation and infrastructure* al ayudar a acercar el conocimiento de la aplicación tecnológica en cuestión a posibles futuros promotores de esta.

En cuanto al comportamiento ético y de responsabilidad social, se considera que el presente trabajo tiene un impacto positivo debido a su contribución para dar a conocer y promocionar el uso de la tecnología planteada para mejorar la seguridad de las comunicaciones, contribuyendo así a mejorar la protección de datos, privacidad y confidencialidad.

Sobre la diversidad, género y derechos humanos, el trabajo se ha elaborado velando por considerar todas las aportaciones en cuanto a referencias, independientemente del género del autor o autora, y el desarrollo realizado es indicado para todos los usuarios con independencia de su género, raza, etc., por lo que no se considera que suponga ningún impacto ni positivo ni negativo en este aspecto.

1.4. Enfoque y método seguido

El presente trabajo está enfocado en el desarrollo de un simulador para distribución de claves cuánticas (*QKD*) mediante comunicación satelital. Para ello el grueso del trabajo se centrará en el análisis e implementación en código del balance de enlace para el canal cuántico, basado en la comunicación mediante señales ópticas. Además, para la implementación de la distribución de claves cuánticas se hará una revisión y adaptación detallada del código propuesto en un trabajo previo [1] para el protocolo *QKD BB84*.

Para conseguir los objetivos marcados, se considera que el mejor método es empezar por el estudio y análisis del funcionamiento del protocolo *QKD BB84* así como del balance de enlace del canal cuántico, identificando en el proceso los parámetros de entrada y salida a utilizar posteriormente en la implementación del simulador, considerando como parámetros de salida aquellos que permiten caracterizar las prestaciones del enlace.
Una vez identificados dichos parámetros y establecida la relación entre ellos, se pretende estructurar el código a implementar en diferentes partes (scripts o funciones) y establecer la relación entre las mismas.
En cuanto al código a implementar, se plantea el uso de MATLAB. Por un lado porque la comunidad educativa, para la cual está pensado el uso del simulador, está familiarizada con este software, y por otra parte porque permite que el código pueda plantearse para ser utilizado mediante una interfaz de usuario, facilitando así el manejo del simulador.

1.5. Planificación del trabajo

Para la realización del trabajo es necesario realizar una búsqueda de recursos que sean de ayuda a nivel de referencia para establecer el marco teórico que permita llegar a una buena implementación en código tanto del protocolo *QKD BB84* como del balance de enlace, y para la implementación en código será necesario el software MATLAB.

Las tareas a realizar, que de forma general se han mencionado en el apartado anterior, van en línea con las metas parciales de cada una de las PECs establecidas, y la planificación temporal de dichas tareas es la mostrada en el siguiente diagrama:

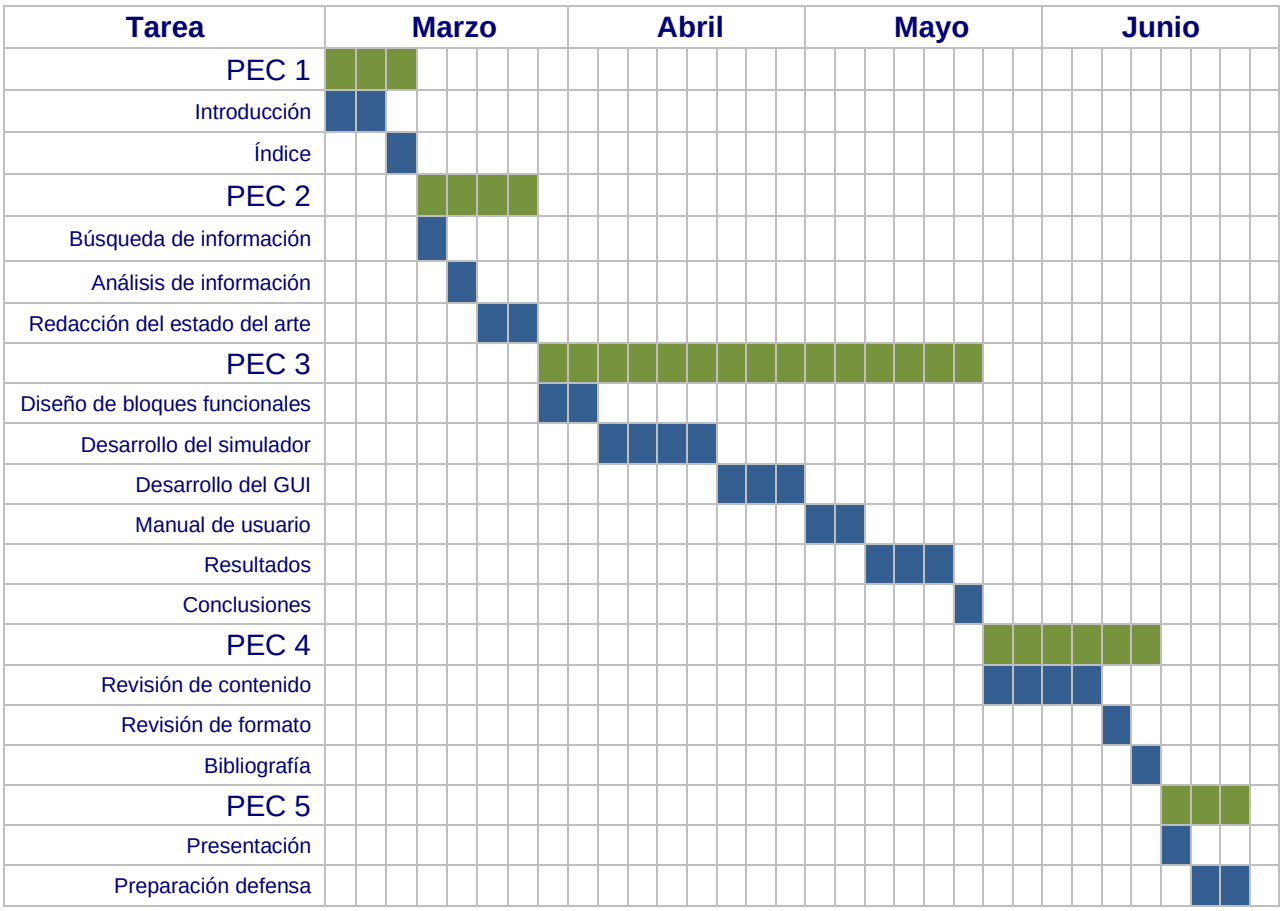

Figura 1: Diagrama de Gantt.

1.6. Breve sumario de productos obtenidos

Como resultado del presente trabajo se obtiene, por una parte, la definición a nivel teórico del protocolo *QKD BB84* implementado junto con un simulador desarrollado en MATLAB que, basado en dicha definición, permite simular el funcionamiento del protocolo. Aunque esta parte se basa en un trabajo previo como punto de partida, las modificaciones y adaptaciones realizadas son considerables, dando lugar a un producto diferente.

Por otra parte, se obtiene como resultado un modelo teórico de canal cuántico para el protocolo *QKD BB84*, basado en la definición teórica del canal cuántico a considerar para una comunicación satelital orientada a *QKD BB84* entre estación terrena y satélite (escenario en enlace descendente, que considera la fuente en satélite). Haciendo uso del modelo obtenido se obtiene un simulador (también desarrollado en MATLAB) que permite parametrizar y analizar el comportamiento del canal cuántico, también bajo la premisa de *QKD BB84*.

1.7. Breve descripción de otros capítulos de la memoria

A continuación se describe de forma breve el contenido de cada uno de los siguientes capítulos:

- Capítulo 2: Tecnologías cuánticas. En este capítulo se describe el estado del arte de las tecnologías cuánticas, definiendo algunos conceptos y fundamentos cuánticos y los objetivos de la comunicación cuántica a largo y corto plazo. El grueso de este capítulo se centra en detallar el estado del arte en cuanto a *QKD*, tanto en general como de forma más concreta en el escenario satelital. En el último apartado se incluye también una recopilación de las herramientas *QKD* existentes.

- Capítulo 3: Comunicación satelital. Es un capítulo en el que se introducen algunos conceptos y fundamentos de la comunicación satelital (como los diferentes tipos de órbitas, el tiempo de visibilidad y las pérdidas en el enlace), y se detalla el balance de enlace a considerar para un canal cuántico orientado a *QKD BB84*, dando lugar al modelo que se usará en el simulador.

- Capítulo 4: Simulador. En este capítulo se detalla el diseño e implementación de cada bloque funcional del código desarrollado, y se incluye un breve manual de usuario del simulador implementado.

- Capítulo 5: Resultados. Es un capítulo en el que se muestran algunos resultados obtenidos haciendo uso del simulador, por una parte del funcionamiento del protocolo *QKD BB84* para diferentes configuraciones de sus parámetros, y por otra del análisis del comportamiento del canal cuántico para *QKD BB84* según la configuración de diferentes variables.

- Capítulo 6: Conclusiones y trabajos futuros. En este capítulo se presentan las conclusiones obtenidas del desarrollo del trabajo y el análisis de resultados, y se plantean diferentes puntos a considerar para trabajos futuros que permitan mejorar o ampliar el alcance del simulador obtenido.

2. Tecnologías cuánticas

Las tecnologías cuánticas han cambiado la forma de pensar sobre la física cuántica, generando un cambio fundamental en la forma en que se entiende la información cuando está codificada en sistemas cuánticos [2].

Aunque están fuertemente interconectados, las áreas de aplicación se basan en cuatro pilares tecnológicos [3]:

- **Computación cuántica** (*QComp*). Se centra en los ordenadores cuánticos de uso general en los que la información cuántica se procesa digitalmente a través de puertas lógicas, de forma similar a los ordenadores clásicos de uso general actuales. Este pilar agrupa muchas capas tecnológicas, desde el procesamiento de información cuántica hasta los algoritmos y aplicaciones finales de estas máquinas. Su objetivo principal es desarrollar dispositivos de computación cuántica que superen o aceleren los ordenadores clásicos existentes para resolver problemas específicos relevantes para la industria, la ciencia y las tecnologías que podrían beneficiare de la ejecución de algoritmos cuánticos.

- **Simulación cuántica** (*QSim*). Este pilar se centra en máquinas con un propósito especial, diseñadas y optimizadas para aplicaciones específicas. En particular, los simuladores cuánticos son dispositivos cuánticos altamente controlables que permiten obtener información sobre las propiedades de los sistemas cuánticos complejos o resolver problemas computacionales específicos que son inaccesibles para los ordenadores clásicos. Se espera que sean aplicables en áreas muy diversas, y además prometen acelerar los casos de problemas de aprendizaje automático, incluidos los núcleos cuánticos y esquemas de clasificación cuántica. Los diferentes enfoques de la simulación cuántica se pueden clasificar en simuladores cuánticos digitales, simuladores cuánticos analógicos, y dispositivos cuánticos heurísticos.

- **Comunicación cuántica** (*QComm*). Su objetivo es diseñar las herramientas y protocolos para intercambiar información cuántica entre usuarios distantes. Dentro de un marco general para las redes de comunicación cuántica, donde el hardware y el software cada vez más complejos dan lugar a funcionalidades más avanzadas, este campo se puede dividir actualmente en dos dominios: por un lado la tecnología a corto plazo, que se centra principalmente en la distribución de claves cuánticas (*QKD*) y otras aplicaciones alcanzables en una etapa similar de funcionalidad a distancias relativamente cortas, habiendo alcanzado un alto nivel de madurez tecnológica e incluso con productos comerciales lanzados al mercado; y por otra parte la investigación y desarrollo a largo plazo para desbloquear todos los beneficios de la comunicación cuántica para usuarios en todo el mundo, permitiendo concretamente la comunicación cuántica a largas distancias y ofreciendo grados de funcionalidad más altos a los usuarios.

- **Metrología y detección cuántica** (*QMS*). Se basan en la explotación de las propiedades cuánticas de la naturaleza, los fenómenos cuánticos, los estados cuánticos, su universalidad y reproducibilidad intrínseca, la cuantización de cantidades físicas asociadas o su alta sensibilidad a los cambios ambientales. Los sensores cuánticos proporcionarán mediciones más precisas en muchos campos, impulsando el rendimiento de los dispositivos y servicios de consumo, desde diagnósticos e imágenes médicas hasta aplicaciones futuras en el Internet de las cosas (*IoT*). Existe una amplia variedad de sensores cuánticos, con propiedades específicas que los hacen adecuados para aplicaciones particulares, aunque el nivel

de madurez según la aplicación es diferente y por tanto hay algunos productos ya disponibles comercialmente mientras que en otros casos aún están en una etapa temprana del desarrollo.

2.1. Conceptos y fundamentos cuánticos

Las tecnologías cuánticas descritas en el apartado anterior se fundamentan en los conceptos de la mecánica cuántica, la cual se basa en considerar que la energía se libera en unidades discretas (partículas) y por tanto la información se transmitirá mediante dichas partículas. Estos conceptos básicos son los siguientes [1]:

- Superposición. Una partícula cuántica (fotón, electrón, etc.) puede hallarse en más de un estado a la vez, coexistiendo de forma simultánea en todas sus posibles configuraciones físicas, y esto se conoce como estado de superposición cuántica.

- Qubit. La unidad básica de medida de la información cuántica es el qubit. A diferencia del bit clásico que sólo existe en uno de los dos estados (0 ó 1), el qubit o bit cuántico puede además presentar superposición de estados y encontrarse en ambos estados a la vez.

- Colapso de estados. La acción de medir una partícula cuántica provoca que se obtenga un resultado de sólo una de sus posibles configuraciones, alterando su estado superpuesto. Es decir, la acción de medir altera el estado superpuesto y hace que la partícula colapse en uno de los posibles estados (0 ó 1).

- Entrelazamiento. Dos partículas cuánticas pueden tener estados correlados entre sí, lo que provoca que la acción de medir una de ellas no sólo haga que esta colapse sino que también determine el estado de la otra partícula.

2.2. Comunicación cuántica

De las tecnologías anteriores, el presente trabajo se centra en la comunicación cuántica, para la cual la visión general es conseguir desarrollar una red cuántica que complemente y amplíe la infraestructura digital actual, sentando las bases para una red de Internet cuántica. Para conseguir este objetivo hay que avanzar en tres direcciones [3]:

- Rendimiento. Aumentar la tasa de qubits, la fiabilidad, la distancia de los enlaces y la solidez de todos los tipos de comunicación cuántica.

- Integración. Combinar la comunicación cuántica con infraestructuras y aplicaciones de red convencionales.

- Industrialización. Realizar tecnología que se pueda fabricar a un precio asequible y que genere riqueza y trabajo.

Objetivo a largo plazo

El objetivo a largo plazo de la comunicación cuántica es disponer de una infraestructura de comunicación cuántica que proporcione una tecnología fundamentalmente nueva al permitir la comunicación cuántica entre dos puntos cualesquiera de la tierra [3].
En sinergia con la red de Internet clásica de la que se dispone actualmente, una red de Internet cuántica conectaría procesadores cuánticos para lograr capacidades incomparables que probablemente son imposibles de alcanzar con la comunicación clásica.
Los componentes claves de dicha red serían los siguientes [3]:

- Repetidores cuánticos. Para conectar muchos usuarios a distancias continentales se puede utilizar un repetidor cuántico para generar entrelazamiento a larga distancia mediante redes de fibra óptica.

- Satélites. Para redes troncales de ultra larga distancia los satélites se pueden usar para hacer la distribución correspondiente entre los diferentes puntos de la red.

- Nodos finales. Son necesarios los dispositivos cuánticos análogos a los actuales ordenadores o teléfonos conectados a Internet para permitir la ejecución de aplicaciones, y por tanto para que la tecnología cuántica de Internet esté disponible para los usuarios finales.

Desde una perspectiva de implementación, la comunicación cuántica requiere del desarrollo de una amplia gama de tecnologías para crear, almacenar y manipular estados cuánticos. El control y manipulación de la luz (fotones), la materia y su interacción son esenciales para lograr una red cuántica segura y por tanto para lograr una red de Internet cuántica. Dichas tecnologías incluyen [3]:

- Fuentes de fotones con propiedades importantes que incluyen requisitos muy estrictos de longitud de onda y ancho de banda, así como especificaciones sobre la pureza y eficiencia.

- Tecnologías de detección de fotones que requieren de mejoras adicionales tanto en el régimen de un solo fotón (*DV-QKD*) como para sistemas de variable continua (*CV-QKD*) [4].

- Memorias cuánticas e interfaces entre portadores de información cuántica (estados cuánticos de luz) y dispositivos de procesamiento y almacenamiento de información cuántica (átomos, iones, sistemas de estado sólido).

Para que todos estos elementos sean realmente útiles, deben construirse con tecnologías que sean escalables a grandes cantidades, y también lo suficientemente resistentes para tolerar los diferentes entornos de uso en la implementación de redes de telecomunicación [3].

Objetivo a corto plazo

Una de las principales aplicaciones de la comunicación cuántica en el corto plazo es el diseño de esquemas criptográficos de seguridad basados en las leyes de la física cuántica [3]. Las comunicaciones seguras desempeñan un papel vital en la economía y la sociedad debido a las grandes cantidades de datos, con diferentes grados de sensibilidad, que se transmiten a diario y son utilizados para realizar operaciones críticas.
Sin embargo, los ordenadores cuánticos representan una amenaza para la criptografía actual, y hay dos alternativas que podrían proporcionar seguridad cuántica [3]:

- La criptografía poscuántica (*PQC*), que aunque no se ocupa de la comunicación cuántica en sí, promete formas de proteger los datos en función de la dureza de construcciones matemáticas específicas.

- La distribución de claves cuánticas (*QKD*), que brinda una seguridad basada en la física cuántica y requiere de comunicaciones cuánticas. El parámetro impulsor de los sistemas *QKD* es la tasa de claves secretas compartidas por los usuarios a través de una distancia determinada.

Aunque estas dos alternativas son diferentes tanto en naturaleza como a nivel de madurez, ambas ofrecen ventajas complementarias pero también deficiencias, por lo que es probable que en un futuro cercano coexistan y se utilicen juntas en un entorno cuántico seguro [3].

La generación de claves *QKD* para el intercambio y almacenamiento seguro de datos requiere de la existencia de canales de comunicación cuánticos, que normalmente forman una red de conexiones ópticas de espacio libre o basadas en fibra. Ambos tipos de canal se han llegado a utilizar con éxito, validando su funcionalidad [3].
A pesar de que los nuevos esquemas han demostrado enlaces *QKD* terrestres de hasta 800 km de longitud, en la práctica el rango de comunicación aún se ve limitado. Para rangos de menos de 100 km se pueden usar conmutadores ópticos y comunicaciones de fibra óptica, y para aumentar más el alcance actualmente y para el corto plazo se usan nodos de retransmisión de confianza. Pero a largo plazo la comunicación cuántica requerirá del desarrollo de repetidores cuánticos, que podrán desarrollarse gracias a la característica cuántica del entrelazamiento (el cual además es la base para la teleportación de qubits) y redes satelitales [3].

Por tanto, aunque actualmente domina el desarrollo de redes *QKD* basadas en el canal de fibra óptica, las limitaciones que supone dicho canal para el rango de la comunicación hacen que el uso del satélite sea una alternativa para tratar de ampliar dicho rango.

2.3. Distribución de claves cuánticas (*QKD*)

La distribución de claves cuánticas es una técnica de criptografía cuántica que permite generar una clave aleatoria compartida por un emisor (típicamente llamado Alice) y un receptor (típicamente llamado Bob) que comparten un canal cuántico, asegurando que ningún tercero (típicamente llamado Eva) tenga opción de obtener dicha clave interceptando el canal de comunicación utilizado en el proceso, ya que siempre se detectaría la presencia de un intruso y entonces se descartaría la clave comprometida [1].

Se trata por tanto de un protocolo mediante el cual emisor y receptor intercambian una serie de qubits codificados en fotones, permitiéndoles a partir de ello acordar una clave secreta [1]. Además, la mayoría de las técnicas *QKD* actuales se basan en la reconciliación de información (corrección de errores) y la amplificación de privacidad (compresión), por lo que se considera que seguirá haciéndose uso de un canal de comunicación clásico, además del canal de comunicación cuántico.

Existen dos variantes principales en la tecnología *QKD*: de variable discreta (*DV-QKD*), basada en el uso de detectores de fotones individuales, y de variable continua (*CV-QKD*), basada en detección coherente. Ambas tienen sus ventajas e inconvenientes; mientras que la primera de ellas permite abordar distancias mayores, la segunda se puede usar en fibras que ya están en uso para la comunicación de datos y el coste de sus componentes es mucho menor. Otra variante es la codificación de referencia de fase distribuida, pero para el presente trabajo se considerarán sólo los *DV-QKD*, que fueron los primeros en inventarse y siguen siendo los más implementados [4].

En la siguiente figura se muestra un esquema básico del sistema de comunicación considerado (en este caso el posible intruso es llamado Kevin):

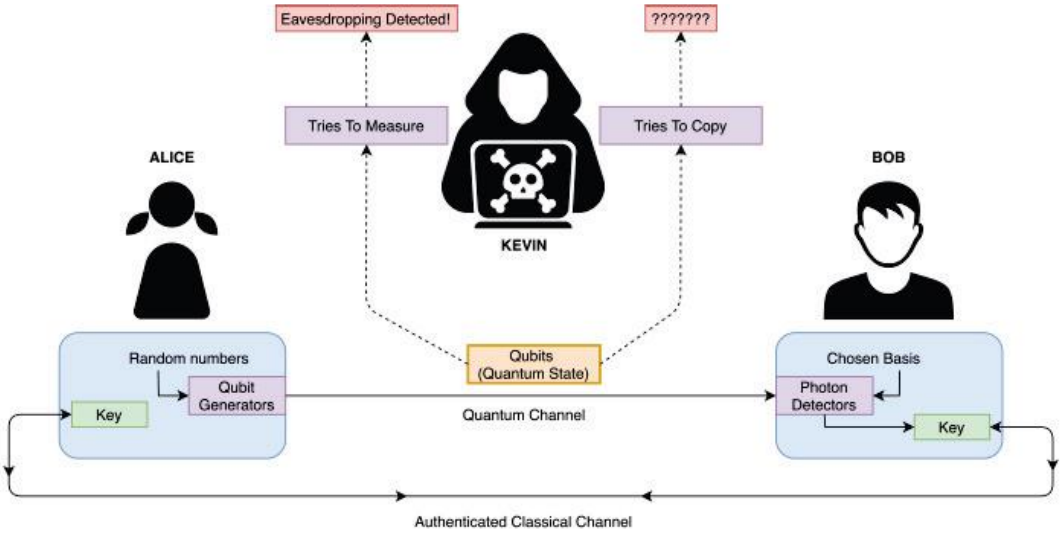

Figura 2: *Flujo básico de QKD* [5].

Puede o no haber presencia del intruso, y en el caso de que lo hubiera entonces la comunicación Alice-Bob sería interceptada por este y entonces el canal cuántico presentaría características diferentes para la comunicación Alice-Intruso y para la de Intruso-Bob, de manera que se considerarían dos canales cuánticos diferentes para dichas comunicaciones [1]:

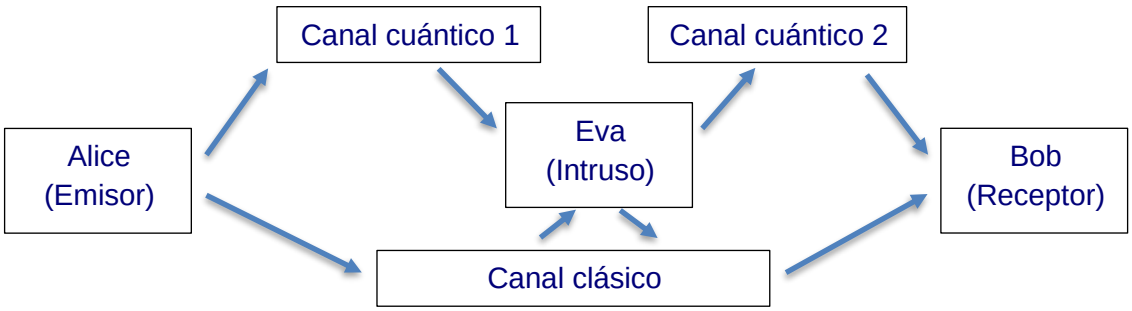

Figura 3: Esquema de comunicación Alice-Bob con intruso, dando lugar a dos canales cuánticos diferentes.

Los pasos seguidos para la generación de la clave cuántica dependen del protocolo concreto que se aplique. Para el presente trabajo se considerará el protocolo *BB84*. En el Anexo I se describe cómo sería el caso del protocolo *BB84*, incluyendo un ejemplo simple. Se puede encontrar una explicación más detallada tanto de este protocolo como de otros en [1].
En la siguiente imagen se presenta un esquema general del intercambio de claves que se realiza entre emisor y receptor para así poder encriptar la información para su transmisión y desencriptarla para acceder a ella:

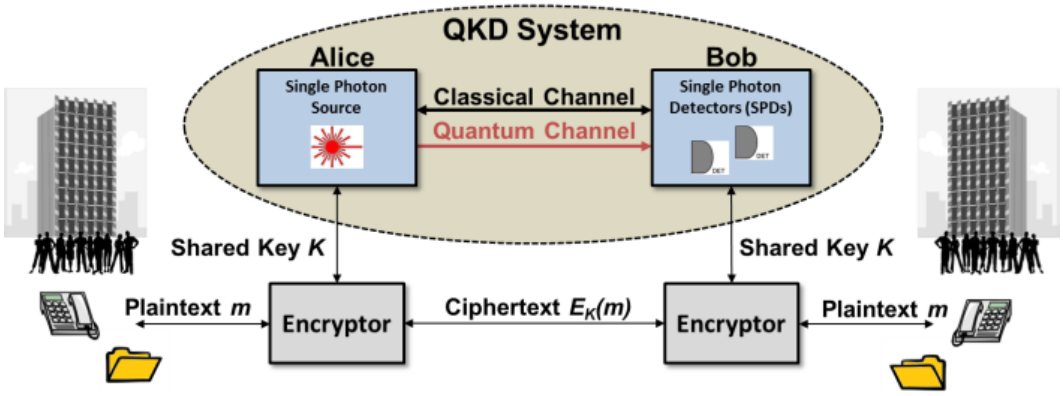

Figura 4: Diagrama de sistema *QKD*. Alice (emisor) y Bob (receptor) generan una clave secreta compartida *K* para encriptar información sensible *[6]*.

Sobre el desarrollo de redes *QKD*, existen ciertas diferencias en cuanto a efectos sobre el canal cuántico dependiendo del propio canal utilizado, aunque el parámetro más importante son las pérdidas. Como se comentaba en el apartado anterior, las implementaciones basadas en fibra óptica presentan ciertas limitaciones para el rango de la comunicación y esto hace que el uso del satélite (canal de espacio libre) sea una alternativa.

Las pérdidas en fibra óptica se deben a procesos de dispersión aleatoria, y por lo tanto dependen exponencialmente de la longitud l [7]:

$$L = 10^{-\alpha l/10}$$

donde el valor de α es fuertemente dependiente de la longitud de onda y es mínimo dentro de las dos ventanas usadas en telecomunicación (para $\lambda = 1330\, nm,\ \alpha \simeq 0.34\, dB/km$, y para $\lambda = 1550\, nm,\ \alpha \simeq 0.2\, dB/km$).
Existen dos efectos principales que modifican el estado de la luz en la fibra óptica [7]:

- Dispersión cromática. Diferentes longitudes de onda viajan a velocidades ligeramente diferentes, dando lugar a una dispersión temporal incoherente de un pulso de luz. Este efecto causa un problema tan pronto como los pulsos siguientes comiencen a superponerse, pero esta dispersión es fija para una fibra dada y se puede compensar.

- Dispersión del modo de polarización (PMD). Un pulso tiende a dividirse en dos componentes ortogonales entre sí, el modo de polarización rápido y el modo de polarización lento. El efecto ocurre cuando las dos componentes recorren la fibra a diferentes velocidades de grupo y así alcanzarán al receptor en tiempos diferentes, induciendo una despolarización del pulso que no puede compensarse estáticamente.

En el caso del enlace satelital (espacio libre) la decoherencia de polarización es prácticamente despreciable, y las pérdidas a considerar se pueden dividir básicamente en [7]:

- Pérdidas geométricas. Están relacionadas con la apertura de los telescopios receptores y con la apertura efectiva del telescopio emisor (la percibida por el receptor está influenciada por el apuntamiento, obstáculos, condiciones atmosféricas, etc.).

- Pérdidas atmosféricas. Se deben a la dispersión y al centelleo. En cuanto a la dispersión, existen varias ventanas de transmisión atmosférica en las que tiene una atenuación de $0.1\, dB/km$ con cielo despejado. Las condiciones meteorológicas influyen mucho en estas pérdidas.

Así, un modelo simple de pérdidas para este canal, de longitud l, vendría dado por [7]:

$$L = \left[\frac{d_r}{d_s + Dl}\right]^2 \cdot 10^{-\alpha l/10}$$

donde el primer término es una estimación de las pérdidas geométricas (con d_s y d_r las aperturas del emisor y receptor, y D la divergencia del haz) y el segundo describe la

dispersión (siendo α la atenuación atmosférica). Téngase en cuenta que este modelo simple no tiene en cuenta el centelleo, que suele ser el factor más crítico en la práctica.
Aunque el anterior es un modelo simplificado, existe literatura como [8], [9] y [10] en la que se describen de forma detallada más efectos y su potencial impacto sobre el canal óptico.

Además, hay que tener también en cuenta que la comunicación cuántica mediante un enlace satelital, en concreto para su aplicación para *QKD*, tiene sus propios retos.
Uno de ellos es el tamaño de los equipos: debido al tamaño limitado de un satélite, el cual debe albergar muchos equipos diferentes para su correcto funcionamiento y mantenimiento en órbita, se hace necesario poder reducir el tamaño de estos lo máximo posible, lo cual supone un reto para la fabricación de equipamiento óptico para comunicación cuántica que permita realmente el despliegue de redes teniendo en cuenta que lo que se ha hecho hasta ahora ha sido de forma experimental.
Otro reto importante es el apuntamiento: para distancias muy grandes, como es el caso de los enlaces espaciales, un factor crítico es conseguir una baja divergencia del haz para que así llegue al receptor la mayor densidad de potencia por unidad de superficie posible. Esto significa que se puede entregar mucha más energía al receptor que en el caso de la radiofrecuencia, donde la longitud de onda es mucho mayor. Pero esta gran directividad del haz requiere de una alta precisión de apuntamiento [8].

Teniendo en cuenta que emisor (Alice) y receptor (Bob) necesitan estar conectados mediante dos canales físicos, uno clásico y uno cuántico, habrá que considerar dos balances de enlace diferentes, uno para cada tipo de canal. Así pues, se tendrá un balance de enlace basado en radiofrecuencia (canal clásico) y otro basado en comunicación óptica (canal cuántico), ambos para comunicación satelital (en espacio libre). Estos balances de enlace se describen en el siguiente capítulo con todo el detalle a considerar para el simulador.

En cuanto a las redes de distribución de claves cuánticas, cabe mencionar las siguientes [11]:

- DARPA. Era una red *QKD* que funcionó de forma continuada durante cuatro años (2004 a 2007, EEUU). Fue un desarrollo realizado de forma conjunta entre algunas empresas y universidades. Admitía una red informática de Internet basada en estándares protegida por distribución de claves cuánticas.

- SECOQC (*Secure Commmunication Based on Quantum Cryptography*). Fue la pirmera red informática del mundo protegida por distribución de clave cuántica (2008). Se basaba en fibra óptica estándar para interconectar seis ubicaciones, usando un total de 200 km de cable de fibra.

- SwissQuantum. Fue el proyecto de mayor duración para probar *QKD* en un entorno de campo (2009-2011). El objetivo principal era validad la fiabilidad y robustez de *QKD* en funcionamiento continuo durante un largo período de tiempo y en un entorno

de campo. La capa cuántica funcionó durante casi dos años hasta que el proyecto se cerró tras cumplir la duración prevista de la prueba.

- Redes chinas. Destaca la misión QUESS, mediante el satélite Mozi/Micius (primer satélite de comunicaciones cuánticas del mundo, 2016), logrando un canal *QKD* con dos estaciones terrestres separadas por 2600 km. Después, junto con una línea de fibra de 2000 km (2017), constituyeron la primera red cuántica espacio-tierra del mundo. Más adelante se prevé que, mediante el uso de 10 satélites, permitirá disponer de una red cifrada cuántica europea-asiática (2020) y una red global para 2030.

- Eagle-1. Se trata de un satélite cuántico que la ESA planea lanzar en 2024 para un sistema experimental de distribución de claves cuánticas basado en el espacio.

QKD en un escenario satelital

Tal y como se ha mencionado anteriormente, el desarrollo de redes *QKD* está bastante avanzado pero tiene limitaciones en cuanto a la distancia a cubrir, por lo que se tiende al desarrollo de *QKD* con el uso del satélite para tratar de paliar esta limitación y así conseguir cubrir mayores distancias evitando además un despliegue terrestre basado en fibra, cuya viabilidad depende además del entorno.
Además, los sistemas actuales de comunicación satelital basados en radiofrecuencia son un cuello de botella para el volumen de datos a transmitir, debido a razones tanto tecnológicas como reglamentarias [8].
Así, la comunicación óptica en el espacio se convierte en una tecnología clave para resolver tanto las limitaciones en el aspecto cuántico para *QKD* como las limitaciones en el aspecto clásico sobre el ancho de banda en comunicación espacial (al mismo tiempo que se reduce el tamaño, peso y potencia de los sistemas de comunicación por satélite y se aprovecha un espectro sin licencia) [8].

La mayoría de los proyectos plantean una visión del satélite en *QKD* como un *trusted-node* (nodo de confianza), y en este escenario el satélite realiza operaciones *QKD* con distintas estaciones terrestres para establecer claves secretas independientes con cada una de ellas. Así, el satélite tiene todas las claves mientras que las estaciones sólo tienen acceso a sus propias claves [12].
Para permitir que dos estaciones compartan una clave común, el satélite combina sus claves respectivas y transmite su paridad bit a bit (que no revela ninguna información útil a posibles intrusos), con lo que cada estación puede recuperar la clave de la otra. Sin embargo, como el satélite tiene todas las claves de todas las estaciones, el acceso a los datos obtenidos por el satélite daría a un intruso el conocimiento completo de la clave [12]. En la siguiente figura se representa este escenario que es tan común en el planteamiento de *QKD* sobre satélite:

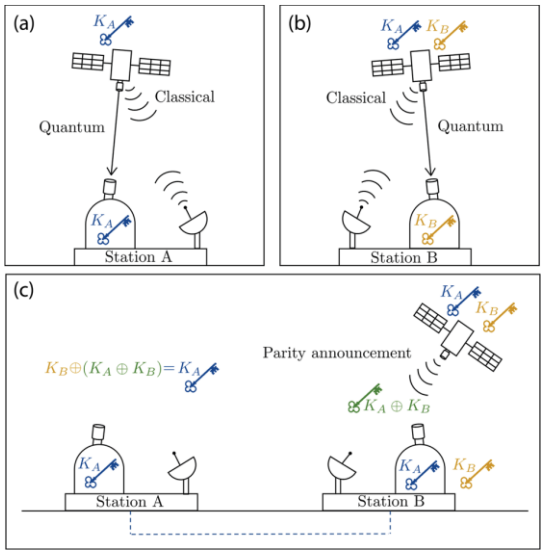

Figura 5: *Esquema más común de QKD sobre satélite como trusted-node* [12].

Sin embargo, la tecnología *QKD* mediante el uso del satélite puede presentar varios escenarios diferentes, los cuales se pueden clasificar según los tipos de enlaces de comunicación que se pueden establecer y la órbita del satélite [12]. Se habla de enlace ascendente cuando la estación terrestre envía señales a un receptor en el espacio, y de enlace descendente cuando es el satélite el que envía las señales a tierra, con lo que existen varias configuraciones posibles para *QKD* con satélites según los tipos de enlaces que se utilicen. Otro tipo de enlace es el intersatelital (*ISL*), que se da cuando un satélite envía señales a otro. Estas configuraciones se muestran en la siguiente figura:

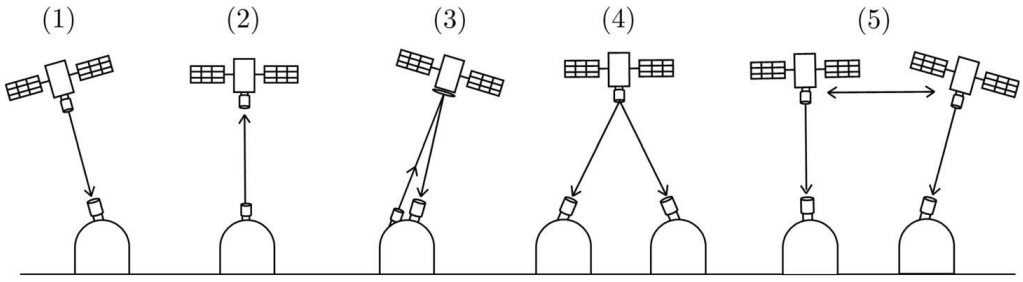

Figura 6: *Escenarios para la implementación de QKD en satélite* [12].

Cada escenario presenta una serie de ventajas e inconvenientes, pero hasta ahora lo recomendado más comúnmente para *QKD* (y el único demostrado hasta ahora) es el uso de enlaces descendentes. Esto es porque presentan pérdidas menores, ya que las propiedades atmosféricas hacen que un transmisor terrestre acabe siendo menos preciso en comparación con un transmisor espacial [12]. Este efecto se puede apreciar de forma ilustrativa en la siguiente representación:

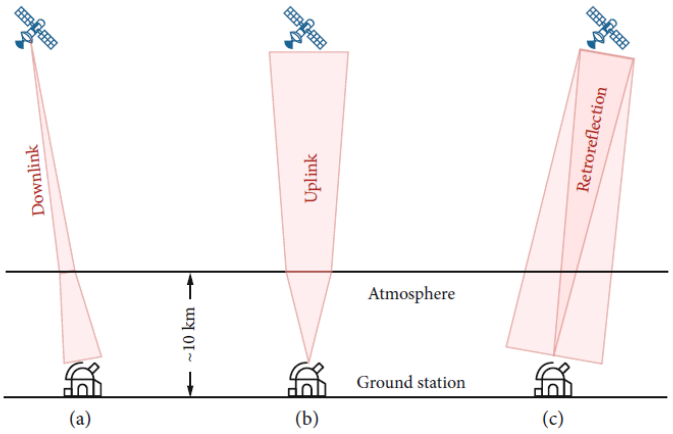

Figura 7: *Configuraciones downlink (a) y uplink (b) de QKD en satélite* [13].

Análisis de herramientas para QKD

Actualmente la mayoría de los simuladores *QKD* sólo admite uno o dos protocolos y además sólo algunos de ellos están disponibles de forma pública para realizar pruebas y análisis. Algunos de estos simuladores se basan en simular solamente los protocolos *QKD*, y otros en la simulación de redes completas *QKD* (protocolos incluidos, como por ejemplo el que se puede encontrar en https://open-qkd.eu/ . En [5] se puede encontrar una recopilación de los principales simuladores desarrollados hasta el momento.

Al ser simuladores experimentales, los primeros son complejos y los segundos se enfocan en la simulación a nivel de capa de red (además de la complejidad de los propios protocolos), por lo que no permiten una fácil adecuación de cara a la comunidad educativa. Sobre el funcionamiento básico de los protocolos sí que existen simuladores online que permiten comprender de forma sencilla su funcionamiento (por ejemplo https://www.st-andrews.ac.uk/physics/quvis/simulations_html5/sims/BB84_photons/BB84_photons.html y https://www.qkdsimulator.com/) pero no están enfocados en el funcionamiento de la comunicación sobre el canal deseado, que en el caso del presente trabajo es el espacio libre mediante el uso de satélites.

Por otra parte, aunque la descripción de algunos simuladores habla tanto de fibra óptica como de espacio libre, están enfocados en el uso del canal de fibra y en el detalle de sus características para la simulación [14], por lo que no existen simuladores que utilicen modelos simples y además se basen en el canal de espacio libre, siendo este uno de los objetivos para el estudio de este tipo de comunicaciones por parte de la comunidad educativa.

Por tanto, aunque hay ya cierto trabajo sobre simuladores *QKD*, no se ha encontrado ninguno comparable con el planteado en el presente trabajo, considerando conceptos básicos tanto a nivel de protocolo como de canal para el estudio de comunicación cuántica *QKD* mediante enlaces satelitales y con orientación educativa.

3. Comunicación satelital

La comunicación satelital tradicional consiste en el uso del satélite como un repetidor situado en una determinada órbita, utilizado tradicionalmente para que una señal de radiofrecuencia transmitida desde una estación terrena que actúa como transmisora pueda ser recibida por otra estación terrena que actúa como receptora, estableciendo así comunicación entre ambas estaciones terrenas a través del satélite.

3.1. Conceptos y fundamentos

Dependiendo de la órbita utilizada y el propio diseño del satélite, este cubrirá determinadas zonas de la tierra que pueden ser fijas o dinámicas y de mayor o menor amplitud.
Una órbita es la trayectoria curvada de un objeto alrededor de un centro de masa, como la de la Tierra alrededor del sol [15].
Las órbitas que describen los satélites alrededor de la Tierra se pueden clasificar en función de diferentes criterios. Uno de ellos es la altura sobre la superficie terrestre, dando lugar a la siguiente clasificación [16] [17]:

- Órbita terrestre baja (*Low Earth Orbit*, LEO). Cuando la altura del satélite sobre la superficie terrestre es de entre 180 km y 2000 km. El satélite tendría un periodo de alrededor de 90 minutos, por lo que el tiempo de visibilidad desde una estación terrena rondaría los 10 minutos en cada pasada [15].
- Órbita terrestre media (*Medium Earth Orbit*, MEO). Cuando la altura del satélite sobre la superficie terrestre es de entre 2000 km y 35786 km. Un satélite que estuviera a una altura de unos 20000 km tendría un periodo de unas 12 horas.
- Órbita geoestacionaria (GEO). Cuando la altura del satélite sobre la superficie terrestre es de 35786 km. Se encuentra en el plano ecuatorial, y como el satélite tendría un periodo igual al de rotación de la Tierra, desde el punto de vista de la Tierra el satélite permanece fijo, cubriendo siempre la misma superficie terrestre.
- Órbita terrestre alta (*High Earth Orbit*, HEO). Cuando la altura del satélite sobre la superficie terrestre es de más de 35786 km. Según la fuente también se puede encontrar definida como órbita altamente elíptica (*Highly Elliptical Orbit*).

Para el presente trabajo sobre la distribución de claves cuánticas se analizará el uso del enlace descendente (satélite-estación terrena) para las órbitas desde LEO a HEO. A pesar de que la órbita HEO no tiene interés para *QKD*, se ha incluido en el simulador por no tener mayor complejidad su inclusión y así poder analizar también cómo sería el comportamiento del canal en ese caso.

Por otra parte, es fundamental entender qué es el tiempo de visibilidad del satélite por parte de la estación terrena (y el tiempo de visibilidad entre satélites para los casos *ISL*). De forma simplificada, el tiempo de visibilidad entre dos cuerpos es aquel durante el cual uno de ellos ve al otro dentro de su campo de visión.

- Como se comentaba anteriormente, en el caso de un satélite en órbita geoestacionaria, una estación terrena que se encuentre dentro de la cobertura de dicho satélite verá que el satélite permanece fijo (órbita E en Figura 8), de manera que dicha estación estará dentro de la cobertura del satélite en todo momento. Una órbita geoestacionaria inclinada es un caso particular en el cual la estación tendrá visibilidad del satélite en todo momento pero para ello tiene que hacer seguimiento (tracking) del mismo, pues no está fijo en un punto pero sí en un área que está dentro del campo de visión de la estación (órbita D en Figura 8).

- Sin embargo, en el caso de un satélite en cualquiera de las otras órbitas (que no son geoestacionarias), una estación terrena que en un determinado momento se encuentre dentro de la cobertura de dicho satélite verá que este se mueve, y con ello también se mueve su cobertura (la zona terrestre que cubre), de manera que dicha estación estará dentro de la cobertura del satélite sólo en determinados periodos de tiempo (órbitas A, B y C en Figura 8). Para aumentar el tiempo de visibilidad en estos casos la estación también tendrá que hacer tracking al satélite mientras este se encuentre dentro de su campo de visión, pero llegará un momento en el que saldrá y ya no habrá visibilidad entre ambos.

Sin entrar en mayor detalle, téngase en cuenta que el tiempo de visibilidad de un satélite dependerá del periodo de su órbita. En la imagen siguiente se muestran los casos ilustrativos que se han ido mencionando antes:

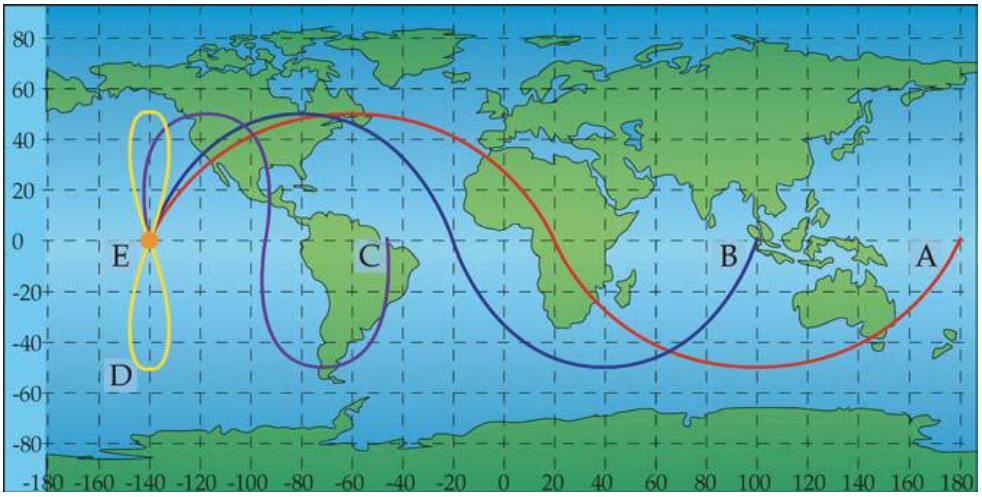

Figura 8: *Visión de diferentes órbitas desde la Tierra. Periodo de órbita A, 2.67 h. Periodo de órbita B, 8 h. Periodo de órbita C, 18 h. Periodo de órbitas D y E, 24 h* [18].

Pérdidas en enlaces satelitales

Para el cálculo de las pérdidas en enlaces satelitales es necesario primero conocer el escenario, ya que no será el mismo para una comunicación entre una estación terrena y un satélite, que entre dos satélites, pero además también dependerá de las condiciones en

cuanto a situación y movimiento de emisor y receptor, a diferencia de la comunicación por fibra óptica en la que simplemente se tienen pérdidas en función de la longitud de la fibra.

Inicialmente hay que ubicar una estación terrena y un satélite, estableciendo un enlace entre ellos que será diferente para los siguientes casos:

- El satélite se encuentra fijo con respecto a la estación terrena y justo sobre ella, en su vertical (el ángulo de elevación de la estación es de 90º). En este caso la distancia total del enlace es igual a la altura del satélite, y la longitud de dicho enlace que pasará a través de la atmósfera corresponde con la altura (grosor) de la propia atmósfera.

- El satélite se encuentra fijo con respecto a la estación terrena y visible desde esta para un ángulo de elevación mayor de 5º (mínimo ángulo de elevación aceptable) y menor de 90º. En este caso la distancia total del enlace es mayor a la altura del satélite, y la longitud de dicho enlace que pasará a través de la atmósfera también es mayor que la altura de la atmósfera. Una variante de este caso es que el satélite no estuviera fijo con respecto a la estación terrena pero sí estuviera visible en todo momento si la estación terrena hace seguimiento del este (ángulo de elevación variable).

- El satélite está en movimiento con respecto a la estación terrena y no es visible desde esta todo el tiempo. En este caso la distancia total del enlace es variable y como mínimo tiene la longitud de la altura del satélite, y la longitud de dicho enlace que pasará a través de la atmósfera también es variable y como mínimo corresponde con la altura de la atmósfera. Además, en este caso, como el satélite no está visible desde la estación terrena, hay que considerar un cierto tiempo de visibilidad entre emisor y receptor.

Por tanto, las pérdidas que sufrirá en enlace dependerán de un efecto atmosférico en función de la distancia recorrida por el enlace a través de la atmósfera, sumado a un efecto en espacio libre (vacío) que también dependerá de la distancia que recorra el enlace en este medio.

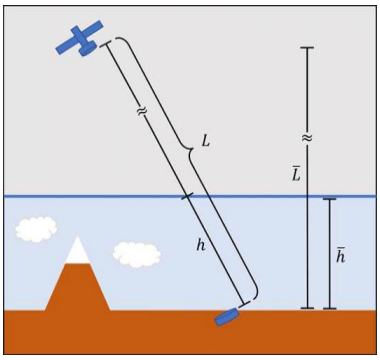

Figura 9: Recorrido del enlace entre estación terrena y satélite por atmósfera y espacio libre [19].

Por otra parte, se tienen los enlaces intersatelitales (*ISL*), para los cuales también puede haber diferentes escenarios dependiendo de la órbita y el movimiento de estos, de forma análoga a los casos descritos entre un satélite y una estación terrena. En este caso la longitud del enlace a través de la atmósfera dependería de las posiciones de los satélites en cada momento, pero se considera que la visibilidad entre dos satélites debe darse evitando la atmósfera (es decir, únicamente a través del vacío).

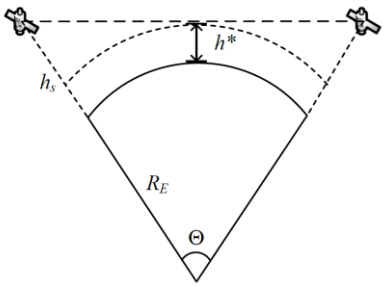

Figura 10: Distancia máxima entre satélites para considerar visibilidad entre ellos [20].

Por tanto, la distancia máxima permitida entre dos satélites para considerar que son mutuamente visibles, y considerando que se encuentran a la misma altitud, vendría dada por la expresión [20]:

$$d^* = 2\sqrt{(R_E + h_s)^2 - (R_E + h^*)^2}$$

donde R_E es el radio medio terrestre, h_s es la altitud de los satélites, y h^* la altitud de la atmósfera.

Es importante en este punto diferenciar entre el tiempo de visibilidad diurno y el tiempo de visibilidad nocturno, ya que para *QKD* se prioriza el uso nocturno para evitar el ruido por irradiación directa solar. Aunque es posible, no es sencillo disminuir la entrada de esta radiación en el sistema óptico y por tanto en el detector, de ahí que el uso de *QKD* suela ser en horarios de visibilidad nocturna.

3.2. Canal cuántico

El canal cuántico a considerar está basado en comunicaciones ópticas, y su balance de enlace (*link budget*) viene dado por la expresión descrita en [8] como:

$$P_R = P_T \cdot G_T \cdot L_T \cdot L_P \cdot L_S \cdot L_A \cdot L_R \cdot G_R$$

donde P_T y P_R son las potencias transmitida y recibida, G_T y G_R son las ganancias del transmisor y el receptor, L_T y L_R las pérdidas del transmisor y el receptor, y L_A, L_P y L_S son las pérdidas atmosféricas, de apuntamiento y de espacio libre, respectivamente.

La ganancia del transmisor viene dada por la expresión $G_T = 16/\Theta_T^2$, siendo $\Theta_T(rad)$ el ángulo de divergencia en transmisión, y la ganancia del receptor viene dada por $G_R = \left(\frac{\pi \cdot D_R}{\lambda}\right)^2$, siendo $D_R(m)$ el diámetro de apertura del receptor.

Por otro lado, las pérdidas atmosféricas vienen dadas por la expresión $L_A = e^{-\alpha_e \cdot l}$, con $\alpha_e = \alpha_a + \alpha_{sc}$ donde α_e es el coeficiente de extinción, α_a el coeficiente de absorción y α_{sc} el coeficiente de *scattering*. Las pérdidas de apuntamiento responden a la expresión $L_P = 10^{\left[-2\left(\frac{\Delta_\Theta}{\Theta_T}\right)^2\right]}$, siendo Δ_Θ la precisión de apuntamiento, y las pérdidas de espacio libre a la expresión $L_S = \left(\frac{\lambda}{4\pi l}\right)^2$, con l la distancia entre terminales (transmisor y receptor).

Sin embargo, para simplificar el modelo se va a considerar que las pérdidas del canal cuántico vienen dadas por la expresión descrita en [7] como:

$$L = \left[\frac{d_R}{d_T + D \cdot l \cdot 1000}\right]^2 \cdot 10^{\frac{-\alpha \cdot l}{10}}$$

en la que el primer término responde a las pérdidas geométricas o de espacio libre y el segundo a las atmosféricas (por dispersión), siendo $d_T\,(m)$ y $d_R(m)$ las aperturas del transmisor y el receptor, $D\,(rad)$ la divergencia del haz, $l\,(km)$ la longitud del enlace, y $\alpha\,(dB/km)$ la atenuación atmosférica. La divergencia total del haz se calcula como $D = 2.44 \cdot \lambda/d_T$ (difracción total por una apertura circular usando el modelo *difraction limited*).

De modo que el balance de enlace quedaría como:

$$P_R = P_T \cdot G_T \cdot L \cdot G_R$$

con $P_T(W)$ y $P_R(W)$ las potencias transmitida y recibida, G_T y G_R las ganancias del transmisor y el receptor, y L las pérdidas del canal.

Téngase en cuenta que la comunicación por un canal cuántico se lleva a cabo haciendo uso de las ventanas de transmisión óptica, pues a pesar de que la mayor parte del enlace se establece en espacio libre, los dispositivos utilizados utilizarán fibra óptica como guía de ondas. Así, las longitudes de onda a considerar serán las siguientes: 850 nm (1ª ventana), 1330 nm (2ª ventana) y 1550 nm (3ª ventana).

Una vez definido el cálculo de las pérdidas a considerar para el canal cuántico, pueden calcularse los parámetros característicos de *QKD* como son el QBER y la tasa de clave secreta (*Secret Key Rate, SKR*).

Para el protocolo *QKD BB84*, la tasa de clave secreta viene dada por la siguiente expresión [21]:

$$R = Q \cdot [1 - f \cdot H_2(e_z) - H_2(e_x)]$$

donde $Q \in [0,1]$ es la ganancia que equivale a la transmitancia del canal (porcentaje de fotones que llegan con respecto al total enviado), f es un parámetro que cuantifica la ineficiencia del proceso clásico de reconciliación de claves, $H_2(x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x)$ es la función de entropía binaria de Shannon, y e_z y e_x corresponden al QBER (Quantum Bit Error Rate) para las bases Z y X.

En cuanto al QBER, aunque hay varios efectos o fuentes de ruido o error por los que se ve afectado, se propone un modelo centrado en el efecto provocado por la probabilidad de *dark count* del detector (probabilidad de detectar un fotón sin que lo hubiera). Se trata de un efecto que está presente en implementaciones reales y que permite considerar un modelo simple pero no tanto como el caso ideal en el que no existiera ruido que afectase al QBER. Teniendo esto en cuenta, se considera que el QBER viene dado por la expresión [22]:

$$e = \frac{s \cdot P_{dark}}{s \cdot \mu \cdot \eta(l) \cdot \eta_{detect} + P_{dark}}$$

donde s es el factor de cribado con valor $s = 0.5$ para *BB84* clásico y $s = 1$ para *BB84* eficiente, P_{dark} es la probabilidad de *dark count* del detector y suele tener valores entre 0.001% y 0.01% [22], μ es la media de fotones contenidos en cada pulso que envía el emisor ($\mu = 1$ para el protocolo *BB84*), $\eta(l)$ es la transmitancia del canal (depende de las pérdidas del canal y por tanto de la longitud del mismo, l), y η_{detect} es la eficiencia del detector.
Es importante tener en cuenta que para el protocolo *BB84* el límite seguro de QBER es del 11% [23], de modo que en caso de superarse dicho umbral la comunicación se vería comprometida y habría que abortar el proceso.

4. Simulador (software MATLAB)

Para el desarrollo del simulador se ha optado por utilizar la herramienta MATLAB, haciendo uso principalmente de la funcionalidad de *Live Script* (también llamada “función en vivo”) que permite combinar código con texto formateado, ecuaciones e imágenes en un entorno único. También se hace uso de funciones clásicas de MATLAB para evitar mostrar código que no sea objetivo directo de estudio en *QKD*, o para evitar mostrarlo repetido tras un primer uso.

Partiendo de estas ideas, a continuación se describe el diseño y la implementación del software en cuestión, así como se presenta un breve manual de usuario para su utilización por parte de la comunidad educativa.

4.1. Diseño

El software propuesto tiene dos objetivos principales: por una parte mostrar el funcionamiento del protocolo *QKD BB84* con una simulación detallada del mismo, y por otra

permitir analizar el comportamiento del canal cuántico para la generación de claves *QKD* mediante *BB84* en función de diferentes parámetros de entrada (incluidos entre ellos el tipo de órbita descrita por el satélite).

Al tratarse de dos objetivos bien diferenciados, y para no confundir al usuario durante la utilización del software, se ha optado por usar un *live script* para cada uno de ellos, dando lugar a los siguientes bloques:

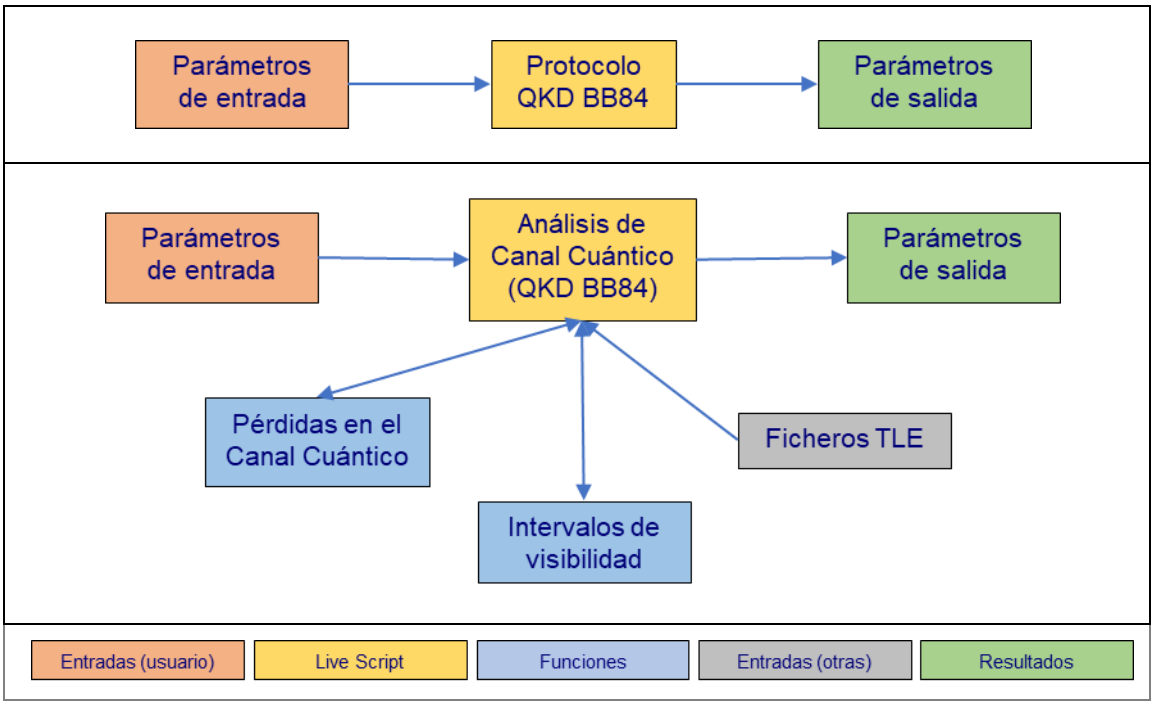

Figura 11: Diseño en bloques del simulador (software MATLAB).

Protocolo QKD BB84

El objetivo es simular el funcionamiento del protocolo en cuanto a comunicaciones y operaciones realizadas entre emisor y receptor para generar una clave secreta, así como obtener métricas de cada ejecución realizada.

- **Parámetros de entrada**: son aquellos que debe introducir el usuario para dar valores a los diferentes parámetros que se utilizarán para simular el funcionamiento del protocolo.
  - Longitud de clave a generar.
  - Pérdidas del canal cuántico (se refiere a pérdidas de fotones).
  - Probabilidad de *dark count* (detección de fotones no existentes).
  - Porcentaje de error permitido entre las bases generadas por emisor y receptor.

- **Protocolo *QKD BB84***: describe el proceso del protocolo en cuanto a comunicaciones y operaciones realizadas por el emisor y el receptor para la generación de una clave secreta.
    - Obtención de parámetros de entrada.
    - Emisor: generación de clave inicial propuesta, generación de bases, y codificación cuántica (fotones). Envío de la clave codificada.
    - Recepción de clave codificada tras aplicar efecto de pérdidas sobre el canal y *dark count* sobre el equipo receptor.
    - Receptor: generación de bases y decodificación de la cadena de fotones recibida, dando lugar a la obtención de clave bruta (*raw key*).
    - Proceso de *sifting*: compartición de bases mediante canal clásico, identificación de posiciones de qubits enviados por el emisor y no detectados por el receptor (*bit sifting*) y descarte de los bits no coincidentes entre las bases (*basis sifting* o reconciliación de bases), dando lugar a la identificación de coincidencias entre las bases.
    - Generación de clave reconciliada preliminar (*preliminar reconcilied key*).
    - Estimación de QBER.
    - Corrección de errores y obtención de clave reconciliada (*reconcilied key*).
    - Amplificación de privacidad y obtención de la clave secreta (*secret key*).

- **Parámetros de salida**: son aquellos que genera el código a partir de los parámetros de entrada dados por el usuario y los cálculos programados.
    - Clave inicial propuesta por el emisor.
    - Bases elegidas por el emisor para codificar la clave inicial.
    - Cadena codificada que envía el emisor (fotones).
    - Cadena codificada que detecta el receptor (fotones).
    - Bases elegidas por el receptor para decodificar la cadena codificada recibida.
    - Cadena decodificada por el receptor (*raw key*).
    - Posiciones en las que las cadenas de bases de emisor y receptor coinciden.
    - Aviso si no se supera el porcentaje de error permitido entre las bases.
    - Clave reconciliada preliminar (*preliminar reconcilied key*).
    - Número de bits reconciliados (preliminar) con respecto al total enviado en la clave inicial.
    - QBER estimado.
    - Aviso si el QBER supera el umbral del 11%. En ese caso se aborta el proceso.
    - Clave reconciliada tras corrección de errores (*reconcilied key*).
    - Comprobación de QBER tras corrección de errores.
    - Número de bits reconciliados con respecto al total enviado en la clave inicial.
    - Eficiencias de reconciliación.
    - Aviso si no hay suficiente material para generar la clave secreta.
    - Clave secreta generada (*secret key*).
    - Eficiencias de generación de la clave secreta.

Análisis de Canal Cuántico para QKD BB84

El objetivo es analizar el comportamiento del canal cuántico para la generación de claves *QKD* mediante *BB84* en función de diferentes parámetros, tomando como base las expresiones teóricas que modelan el canal para este protocolo concreto.

- **Parámetros de entrada**: son aquellos que debe introducir el usuario para dar valores a los diferentes parámetros que se utilizarán para analizar el comportamiento del canal.
    - Longitud de onda mediante elección de ventana óptica de transmisión.
    - Diámetro de apertura del transmisor.
    - Diámetro de apertura del receptor.
    - Atenuación atmosférica.
    - Longitud total del enlace (para configuración manual del escenario).
    - Longitud del enlace a través de la atmósfera (para configuración manual del escenario).
    - Tiempo diario de visibilidad del satélite (para configuración manual del escenario).
    - Fecha y hora de inicio de la simulación (para configuración con TLE).
    - Duración de la simulación en días (para configuración con TLE).
    - Latitud y longitud de la estación terrena (para configuración con TLE).
    - Tipo de *BB84* (clásico o eficiente).
    - Probabilidad de *dark count*.
    - Eficiencia del detector.
    - Frecuencia de uso del canal.
    - Opciones para generación de gráficas.

- **Análisis de Canal Cuántico (*QKD BB84*)**: describe los cálculos para analizar el comportamiento del canal en valores numéricos de pérdidas, QBER y tasa de clave secreta.
    - Obtención de parámetros de entrada.
    - Cálculo de pérdidas totales.
    - Cálculo de QBER.
    - Cálculo de tasa de clave secreta.
    - Cálculo de tasa diaria de generación de claves secretas.
    - Generación de gráficas en función de diferentes parámetros (según elección del usuario).

- **Pérdidas en el Canal Cuántico**: función que calcula las pérdidas totales del canal cuántico dados los parámetros de entrada necesarios. Se utiliza para la generación de gráficas para evitar repetir código.

- **Intervalos de visibilidad**: función que calcula los intervalos de visibilidad entre un satélite y una estación terrena. La entrada de la función es un fichero TLE (*Two Line*

Elements), la fecha y hora de inicio y la duración en días para simular el escenario, y la latitud y longitud de la estación terrena. Entre los valores que devuelve, además de los intervalos de visibilidad como tal, están el rango del satélite, el ángulo de elevación de la estación terrena y un escenario que permite la visualización en video del movimiento del satélite con respecto a la posición de la estación terrena.

- **Ficheros TLE**: son ficheros con un formato de datos que codifica una lista de parámetros orbitales de un cuerpo en órbita terrestre para un momento determinado. Se proporciona un fichero por cada tipo de órbita (LEO, MEO, GEO y HEO) obtenidos de [24].

- **Parámetros de salida**: son aquellos que genera el código a partir de los parámetros de entrada dados por el usuario y los cálculos programados.
  - Pérdidas totales del enlace.
  - Transmitancia del canal.
  - QBER.
  - Tasa de clave secreta.
  - Tasa diaria de generación de claves secretas.
  - Comparación gráfica de tasa diaria de generación de claves secretas para diferentes tipos de órbitas.
  - Representación gráfica de pérdidas, QBER y tasa de clave secreta en función de diferentes parámetros.

4.2. Implementación

La implementación del software consiste en la generación de los dos *live scripts* descritos en el apartado anterior, que incluyen tanto explicaciones para el usuario como código para realizar los cálculos necesarios y obtener los resultados. A continuación se detalla la implementación de cada uno de ellos, teniendo en cuenta las premisas tomadas en cada caso.

Protocolo QKD BB84

El objetivo de este *live script* es simular el funcionamiento del protocolo en cuanto a comunicaciones y operaciones entre emisor y receptor para generar una clave secreta, así como obtener métricas de cada ejecución realizada. El fichero generado es *QKD_BB84_Protocol.mlx*.

Inicialmente se ha considerado un funcionamiento simplificado del protocolo en el que no hay intervención de ningún intruso, presentando entonces un único canal entre emisor y receptor (no hay configuración del “doble canal” que se daría al tener un intruso, pero sí se incluye un parámetro para indicar el número de bits que podrían verse comprometidos si se interceptase la comunicación).

Aun así, ha sido necesario realizar bastantes modificaciones en el código que se tenía inicialmente [1] para poder simular de forma adecuada el efecto tanto de las pérdidas del canal como de *dark count*.

1. **Configuración de la comunicación cuántica entre emisor (Alice) y receptor (Bob).**
   En este apartado se pueden configurar los principales parámetros de entrada, aunque ya se establecen con unos valores por defecto. Dichos parámetros son la longitud de la clave a generar (en bytes, que luego se traduce a bits en el código), las pérdidas del canal cuántico como probabilidad de pérdida de fotones, y la probabilidad de *dark count* en el receptor.

2. **Alice: generación de clave inicial, generación de bases, y codificación cuántica (fotones).**
   En este apartado no hay intervención del usuario, sino que haciendo uso de los parámetros anteriormente definidos y las generaciones aleatorias de secuencias de bits, se exponen al usuario la secuencia de bits de la clave inicial (A1), la secuencia de bits que representa la elección de las bases para la codificación cuántica (A2), y la secuencia de qubits generada tras codificar A1 con A2 (A).

3. **Recepción de clave codificada tras aplicar efecto de pérdidas sobre el canal y *dark count* sobre el equipo receptor.**
   Tampoco hay intervención del usuario en este punto. Teniendo en cuenta las pérdidas del canal (que suponen pérdida de fotones) y el efecto de *dark count* en el receptor (que supone detección de fotones inexistentes), se genera la secuencia de qubits que detectaría el receptor, indicando aquellas posiciones de la secuencia que estarían vacías por la pérdida del fotón a través del canal. En el caso del efecto de *dark count*, cuando hay detección de fotones por este efecto se les asigna un valor 0 o 1 de forma aleatoria.

4. **Bob: generación de bases y decodificación de la cadena de qubits detectada - (*Raw Key*).**
   De nuevo no hay intervención del usuario en este apartado. Una vez generada la secuencia de qubits que detectaría el receptor, este genera una secuencia aleatoria de bases para decodificarla, dando lugar a la clave bruta sin procesar (B1) conocida como *Raw Key*.

5. **Reconciliación de bases.**
   En este punto el emisor compartiría con el receptor su secuencia de bases (A2) mediante el canal clásico, y el receptor le respondería con las posiciones en que coincide con la suya (B2). El usuario puede configurar qué porcentaje mínimo de coincidencias deben existir entre las secuencias de bases para considerar que el proceso sería válido (aunque no es determinante, pues se muestra un aviso en caso de no cumplirse pero se permite seguir con el proceso). Como resultados se

muestran las posiciones en que B2 y A2 coinciden, así como el número total de bits coincidentes con respecto a la longitud de las secuencias.

6. **Generación de clave reconciliada preliminar - (*Preliminar Reconcilied Key*).**
   En este apartado, a partir de la reconciliación de bases, tanto emisor como receptor generan una clave reconciliada preliminar, quedándose con los bits de su *raw key* para los cuales las bases hayan coincidido. Como resultado se muestran al usuario dichas claves reconciliadas preliminares, así como el número de bits reconciliados con respecto al total enviado inicialmente.

7. **Estimación de QBER.**
   En este punto se realiza el cálculo del QBER obteniendo las diferencias entre las claves reconciliadas preliminares con respecto a la longitud de A1 (sin tener en cuenta los fotones perdidos, que no son errores sino pérdidas). En el proceso real, emisor y receptor compartirían una parte de sus claves reconciliadas preliminares para realizar una estimación del QBER, pero al tratarse en este caso de una simulación se ha simplificado el proceso haciendo un cálculo directo de este parámetro dado que disponemos de ambas secuencias. En el caso de que el QBER obtenido sea superior al 11%, se mostrará un aviso al usuario indicando que la clave está comprometida y que por tanto debe abortarse el proceso.

8. **Corrección de errores y obtención de clave reconciliada - (*Reconcilied Key*).**
   En este punto se describe en qué consiste el proceso de corrección de errores, que dará lugar a una reducción del tamaño de la clave reconciliada preliminar en un factor de ineficiencia del proceso (f), configurable por el usuario. La corrección de errores aplicada, tomando la ventaja de que se trata de una simulación, se ha llevado a cabo eliminando aquellos bits en los que las claves reconciliadas preliminares no coinciden, y posteriormente se terminan de acortar (cuando corresponda) para cumplir con el factor de reducción f que se haya configurado, dando lugar a la *Reconcilied Key*. Téngase en cuenta que en el proceso real la corrección de errores se haría compartiendo parte de las claves reconciliadas preliminares. Como resultados se muestran al usuario las claves reconciliadas tras el proceso de corrección de errores, el número de bits reconciliados frente al total que se habían enviado inicialmente, el QBER calculado de nuevo tras la corrección de errores (que se espera que sea nulo puesto que ya no tendría que haber errores), y también datos sobre la eficiencia de reconciliación (cuánta *raw key* efectiva se tiene tras la reconciliación, y cuál sería la eficiencia global comparando con el número de bits de la clave inicial).

9. **Ampliación de privacidad y obtención de la clave secreta - (*Secret Key*).**
   Por último, se explica al usuario en qué consiste la generación de la clave secreta mediante la aplicación del proceso de amplificación de privacidad (que resultará en una clave aún más reducida), permitiendo que este pueda ajustar el número de bits que podrían verse comprometidos (conocidos por un posible intruso). En caso de que

no haya suficientes bits (de la *reconcilied key*) para obtener una *secret key*, se indicará al usuario que no hay suficiente material para generar una clave secreta. Si se ha podido generar la clave secreta, entonces como resultados se mostrarán la propia *Secret Key*, y también cálculos sobre la eficiencia de esta (cuánta *reconcilied key* efectiva se tiene tras la generación de la clave secreta, y cuál sería la eficiencia global comparando con el número de bits de la clave inicial).

Análisis de Canal Cuántico para QKD BB84

El objetivo de este *live script* es analizar el comportamiento del canal cuántico para la generación de claves *QKD* mediante el protocolo *BB84* en función de diferentes parámetros, tomando como base las expresiones teóricas que modelan el canal para este protocolo, y dando lugar a resultados tanto numéricos como gráficos. El fichero generado es *QKD_BB84_QChannel.mlx*, el cual hace uso de los ficheros TLE (*LEO.txt*, *MEO.txt*, *GEO.txt*, *HEO.txt*), y de las funciones *lossesQuantumChannel.m* y *visibilityIntervals.m*.

Téngase en cuenta que los ficheros TLE proporcionados como referencia son de satélites reales, por lo que podrían utilizarse otros diferentes si se quiere analizar algún otro caso concreto.

1. **Cálculo de las pérdidas del canal.**
   En este apartado se detalla la expresión que modela las pérdidas del canal y se configuran los parámetros de entrada para poder realizar el cálculo. Permite elegir entre una configuración manual de los parámetros, o una configuración parcial en la que en caso de elegir un determinado tipo de órbita se hace uso del fichero TLE correspondiente y la función *visibilityIntervals.m* para obtener los intervalos de visibilidad y las diferentes características del enlace (rango y distancia a través de la atmósfera). Se ofrece la opción de visualizar el escenario real del movimiento de dicho satélite con respecto a la estación terrena con la ubicación definida. Como resultado se obtienen las pérdidas totales del enlace, y se da la opción de representar gráficamente la contribución de las geométricas y atmosféricas a las totales.

2. **Cálculo del QBER.**
   En este apartado se detalla la expresión de QBER para el protocolo *BB84* y se configuran los parámetros necesarios para el cálculo. Para simplificar el análisis se toma como premisa que el QBER sea igual independientemente de si la base es Z o X. Como resultado, además del QBER, se muestra también la transmitancia del canal (que corresponde con la inversa de las pérdidas calculadas en el apartado anterior pero se muestra aquí porque es donde interviene).

3. **Cálculo de la tasa de clave secreta por uso del canal.**
   Aquí se detalla la expresión de la tasa de clave secreta para el protocolo *BB84*. Se puede calcular sin necesidad de definir más parámetros que los ya definidos en los apartados anteriores. El resultado es una tasa de clave secreta por uso de canal.

4. **Cálculo de la tasa de clave secreta.**
   Como en el apartado anterior el resultado era una tasa de clave secreta por uso de canal, en este punto se permite al usuario definir una frecuencia de uso del canal para calcular una tasa diaria de clave secreta. Para ello es además necesario el tiempo total de visibilidad diaria entre satélite y estación terrena, por lo que en el caso de haber elegido la opción manual en el primer apartado, el usuario también tendrá que definir este tiempo. Sin embargo, si se ha elegido algún tipo de órbita concreta, este tiempo de visibilidad se obtendrá a partir de los resultados que haya devuelvo la función *visibilityIntervals.m*.

5. **Comparativa de tasa diaria de generación de claves secretas para diferentes tipos de órbitas.**
   En este apartado se permite al usuario ver gráficamente una comparativa de la tasa diaria de claves secretas para cada uno de los tipos de órbita considerados (LEO, MEO, GEO y HEO) en función de la frecuencia de uso del canal. Para ello se define un vector de valores para la frecuencia de uso del canal, y para cada uno de los tipos de órbitas se va calculando la tasa diaria de generación de claves secretas para cada valor de la frecuencia de uso. Se utilizan en este apartado las funciones *visibilityIntervals.m* y *lossesQuantumChannel.m* para evitar más líneas de código en el *live script*. Para el resto de los datos, se consideran los que se hayan definido en los apartados anteriores.

6. **Generación de gráficas de pérdidas, QBER y tasa de clave secreta.**
   En este último apartado se permite al usuario generar gráficas de pérdidas totales, QBER y tasa de clave secreta por uso de canal en función de diferentes parámetros. Para ello, una vez que el usuario elije el parámetro en función del cual quiere hacer la representación, se crea un vector de valores para dicho parámetro y se hacen los cálculos correspondientes para cada uno de ellos. De nuevo se hace uso de la función *lossesQuantumChannel.m*. Además, excepto para las representaciones que son en función de las aperturas de emisor y receptor (que se representan en 3D para comparar los resultados en función de ambas aperturas), en el resto de los casos se incluye por defecto la comparativa entre las diferentes longitudes de onda correspondientes a las ventanas ópticas de transmisión.

4.3. Manual de usuario

El uso de *Live Script* es muy intuitivo, por lo que el manual de usuario descrito está en general más enfocado al uso y configuración de la vista de *live scripts*, aunque se detallan también aspectos específicos sobre el uso del software implementado.

Ejecución de LiveScripts en MATLAB

Un *Live Script* o función en vivo es un tipo de *script* que permite combinar código con texto formateado, ecuaciones e imágenes en un entorno único.

El software desarrollado consta de dos *Live Scripts*:

- *QKD_BB84_Protocol.mlx*
- *QKD_BB84_Qchannel.mlx*. Este hace uso de las dos funciones desarrolladas *lossesQuantumChannel.m* y *visibilityIntervals.m*, y también de los cuatro ficheros TLE proporcionados.

Se recomienda poner todos los ficheros proporcionados en el mismo directorio de MATLAB y desde el mismo abrir el *Live Script* que quiera usarse. De esta forma, sea cual sea el que se vaya a utilizar, las funciones y ficheros necesarios estarán en el mismo directorio y por tanto accesibles.

Una vez abierto el *Live Script* deseado en *MATLAB*, vaya a la pestaña *VIEW* de la barra superior y verá varias opciones:

- *DISPLAY*: la opción *Datatips* es útil sólo en el caso de quiera analizarse el funcionamiento del código implementado, pues una vez que se han realizado cálculos y teniendo el código visible, permite ver cuál es el valor de las diferentes variables al poner el cursor sobre una de ellas.

Figura 12: Opción *Datatips*.

- *OUTPUT*: una vez realizada alguna ejecución del código, la opción *Clear All Output* permite eliminar todas las salidas calculadas por el mismo.

- *VIEW*: aquí se muestran tres posibles opciones para visualizar tanto el *Live Script* en sí como los resultados que genera.
  - *Output on Right*. Permite visualizar a la izquierda de la pantalla el *Live Script* (con el código visible) y a la derecha las salidas que genera. Para cambiar el valor de los parámetros de entrada, aunque se haya insertado una entidad de

control para facilitar el uso, estas se encuentran dentro de las secciones de código, dificultando la identificación de los parámetros a configurar. Por defecto las salidas se muestran a la misma altura de la línea de código que las genera, y conforme se hace *scroll* en la parte del Live Script también se hace en la parte de las salidas. Para tener el mayor número de salidas a la vista se recomienda, en caso de elegir esta vista, desactivar el *scroll* síncrono (para ello se hace clic con el botón derecho en la parte de visualización de las salidas y se clica sobre *Disable Synchronous Scrolling*.

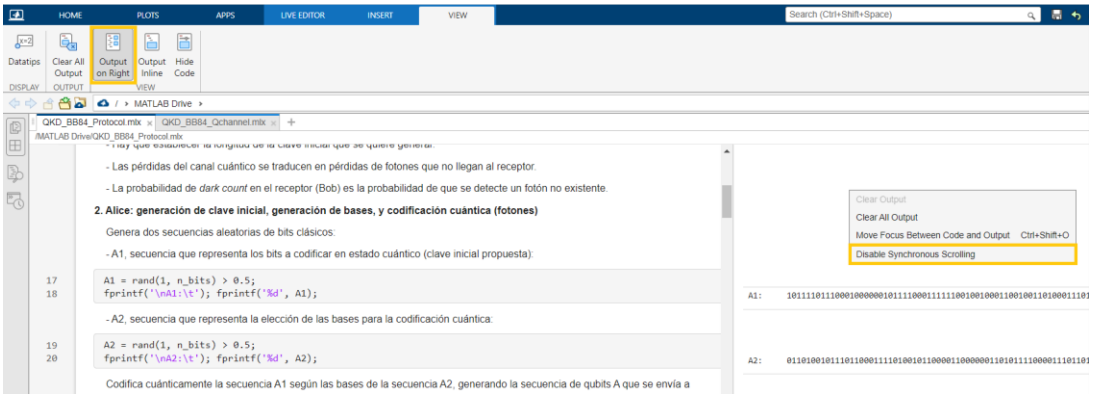

Figura 13: Desactivar opción de *scroll* síncrono.

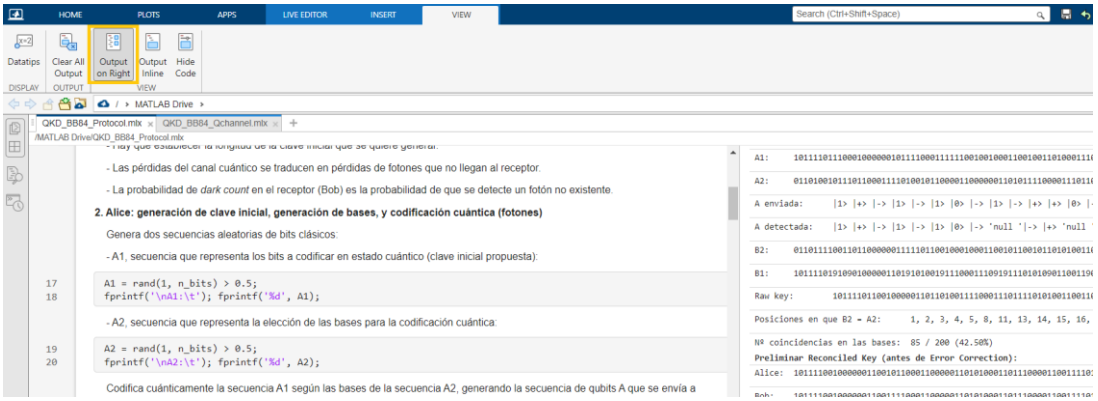

Figura 14: Vista de *Live Script* con resultados a la derecha.

- *Output Inline*. Permite visualizar en la misma parte de la pantalla tanto el contenido del *Live Script* (con el código visible) como las salidas que genera, mostrando estas justo tras el código que las haya generado. Para cambiar el valor de los parámetros de entrada, aunque se haya insertado una entidad de control para facilitar el uso, estas se encuentran dentro de las secciones de código, dificultando la identificación de los parámetros a configurar.

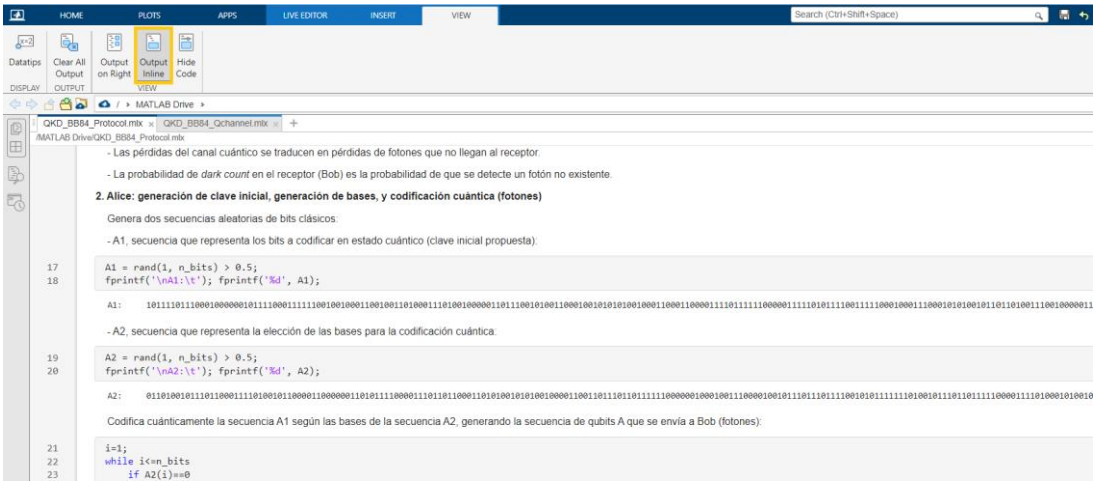

Figura 15: Vista de *Live Script* con resultados en línea.

- *Hide Code*. RECOMENDADO. Permite visualizar en la misma parte de la pantalla tanto el contenido del *Live Script* (con el código oculto) como las salidas que genera, mostrando estas justo tras el código que las haya generado, pero al estar el código oculto es el tipo de visualización más parecido a un típico interfaz de usuario. Para cambiar el valor de los parámetros de entrada, se muestran las entidades de control junto con su descripción, facilitando la identificación de los parámetros a configurar. Es la opción recomendada para utilizar los *Live Scripts* desarrollados en este trabajo (siempre y cuando no se requiera ver el detalle del código).

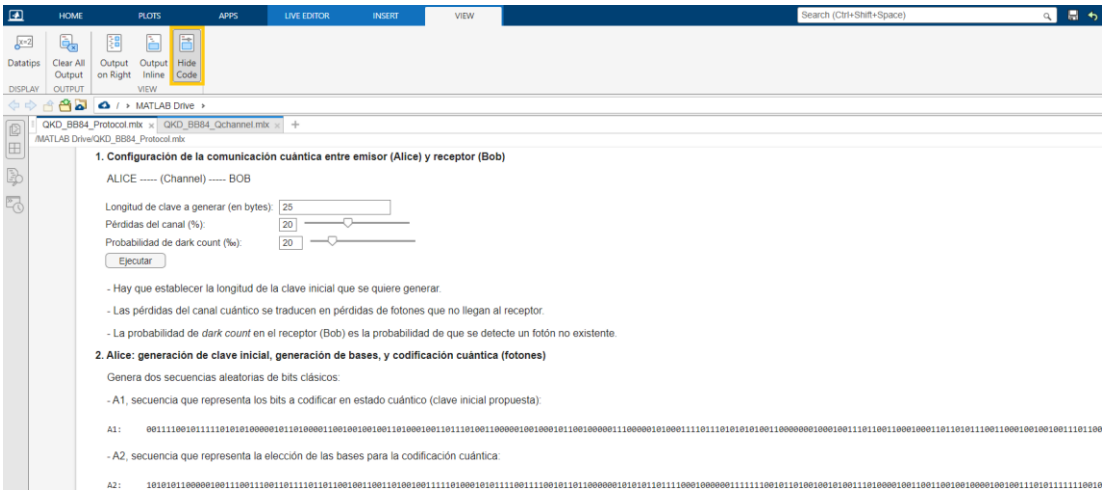

Figura 16: Vista de *Live Script* con código oculto.

Protocolo QKD BB84

El Live Script *QKD_BB84_Protocol.mlx* sirve para simular el funcionamiento del protocolo *QKD BB84* en lo que se refiere a comunicaciones y operaciones realizadas entre el emisor y el receptor para generar una clave secreta.

Para su utilización, una vez abierto el fichero en *MATLAB*, el usuario debe ir leyendo el contenido del mismo y configurando los diferentes parámetros que se muestran. Tras una primera ejecución entendiendo lo que se describe, el usuario podrá realizar todas las ejecuciones que sean necesarias para diferentes configuraciones de los parámetros.

Sólo existe un botón *Ejecutar* que se encuentra en el primer punto del *Live Script*, tras los campos de configuración de los principales parámetros de entrada, y que aplica sobre el conjunto completo del *Live Script*. Aunque en otros puntos también hay algunos campos configurables, si se modifica alguno de ellos las salidas afectadas se volverán a calcular de forma automática. Por tanto, sólo es necesario clicar en el botón de *Ejecuta*r en caso de que se hayan modificado los campos configurables que hay antes del propio botón.

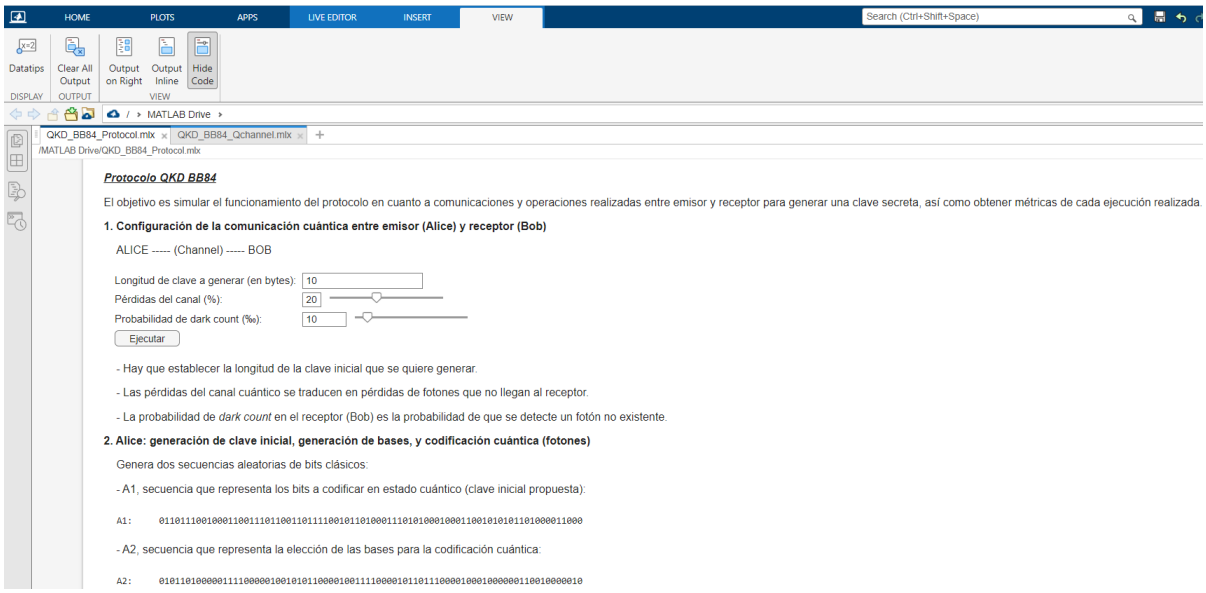

Figura 17: Vista parcial del *Live Script QKD_BB84_Protocol.mlx*.

Téngase en cuenta que aunque la probabilidad de *dark count* suele tener valores entre 0.01‰ y 0.1‰, el rango de valores propuesto para la selección por parte del usuario es mayor (hasta el 100‰), pues al tratarse de una probabilidad tan pequeña sería muy poco probable observar el efecto para una longitud de clave relativamente pequeña, y lo que se pretende es que el usuario pueda observar qué efecto tiene el *dark count* sobre los resultados.

Análisis de Canal Cuántico para QKD BB84

El Live Script *QKD_BB84_Qchannel.mlx* sirve para analizar, en función de diferentes parámetros, el comportamiento del canal cuántico de cara a la generación de claves *QKD* mediante el uso del protocolo *BB84*.

Para su utilización, una vez abierto el fichero en MATLAB, el usuario debe ir leyendo el contenido de este y por cada apartado configurar los parámetros que se muestran y lanzar el cálculo para visualizar los resultados correspondientes.

En este caso, aunque los diferentes apartados están relacionados por algunos parámetros (dependiendo de las opciones elegidas), hay un botón *Calcular* para cada apartado que lanza los cálculos para mostrar los resultados del apartado en cuestión, y también un botón *Ejecutar todo* que lanza los cálculos para todos los apartados. Si se va siguiendo el orden del Live Script, se recomienda utilizar el botón *Calcular* de cada apartado, pero una vez que el usuario conozca el contenido de cada apartado puede ser más cómodo el uso del botón Ejecutar todo para no tener que estar volviendo al principio y ejecutando cada apartado por separado y en orden.

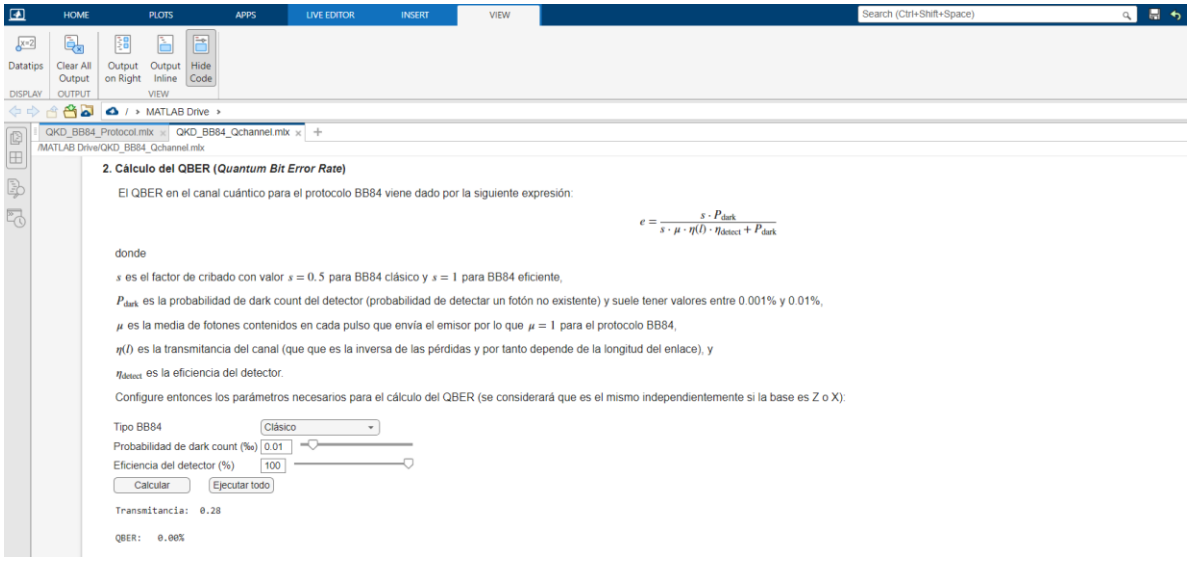

Figura 18: Vista parcial del *Live Script QKD_BB84_QChannel.mlx*.

Téngase en cuenta que, para cada intervalo de visibilidad, la función *visibilityIntervals.m* calcula el tiempo (fecha y hora) medio y para dicho momento los ángulos de azimut y elevación, el rango del satélite, la posición del satélite, y la longitud del enlace a través de la atmósfera. Además se indica cuáles de esos intervalos tienen un "uso permitido", para lo cual se pone como restricción que el ángulo de elevación debe ser mayor de 5º. Una vez obtenidos estos resultados que da esa función, en el LiveScript se calculan la longitud media del enlace (media de los rangos del satélite), la longitud media del enlace a través de la atmósfera y el tiempo total de visibilidad, todos ellos considerando únicamente los intervalos de uso permitido. Esos intervalos de uso permitido son los que se visualizan en la salida del Live Script (los de uso no permitido no se muestran).

5. Resultados

Tras la implementación del software descrito, en este apartado se muestran y comentan algunos de los resultados obtenidos mediante el uso de este tras realizar varias simulaciones con diferentes configuraciones.

5.1. Protocolo *QKD BB84*

A continuación se presentan los resultados obtenidos para diferentes configuraciones de los parámetros de entrada. Téngase en cuenta que para una misma configuración, cada ejecución dará resultados diferentes debido a la aleatoriedad intrínseca que existe en el protocolo.

- Se considera la siguiente configuración del canal (sin pérdidas y sin efecto de *dark count*, y además sin bits comprometidos):

Parámetro	**Valor**
Longitud de clave a generar (bytes)	10
Pérdidas del canal (%)	0
Probabilidad de *dark count* (‰)	0
Factor de reducción de la *Preliminar Reconcilied Key*	1.15
Nº de bits comprometidos	0

Tabla 1: Configuración propuesta 1 para protocolo *QKD BB84*.

Obteniéndose las siguientes salidas:

- A1, secuencia que representa los bits a codificar en estado cuántico (clave inicial propuesta):

```
A1:     01000000010011000010111111100010111110010001110110101100101001111011110111001001
```

- A2, secuencia que representa la elección de las bases para la codificación cuántica:

```
A2:     10001111000011111101001100110000001001100101110011010111010100101110000101101111
```

- B2, secuencia que representa la elección de las bases para la decodificación cuántica de los qubits recibidos:

```
B2:     00110010010100110111011100001000101000100110110011001110111000110111001001011000
```

Decodifica la cadena de qubits detectada (la mide haciendo uso de las bases B2), dando lugar a la secuencia de bits clásicos:

- B1, secuencia decodificada para obtener A1 (el valor "9" indica "fotón perdido"):

```
B1:     11110101000011001000011011000010110110111001110110101110101101111011110011001010
```

Por tanto, la clave "bruta" (sin procesar) sería:

```
Raw key:        11110101000011001000011011000010110110111001110110101110101101111011110011001010
Nº coincidencias en las bases:  42 / 80 (52.50%)
```

Alice genera la clave reconciliada preliminar: se queda con los bits de A1 para los que ha coincidido con las bases de Bob:

```
Alice:  10000001110001111010011011010010111011111
```

Bob genera la clave reconciliada preliminar: se queda con los bits de B1 para los que ha coincidido con las bases de Alice:

```
Bob:    10000001110001111010011011010010111011111
Bits reconciliados:     42 / 80 del total enviado inicialmente
QBER:   0.00%
```

```
Reconciled Key (tras el proceso Error Correction)

Alice:  00111000111101001101101001011101111111

Bob:    00111000111101001101101001011101111111

Bits reconciliados:     37 / 80 del total enviado inicialmente
```

- Se mide cuánta *Raw Key* efectiva se tiene tras la reconciliación:

```
Eficiencia reconciliación:      46.25%
```

- Y cuál sería la eficiencia global comparando con el número de bits de la clave inicial:

```
Eficiencia reconciliación global:       46.25%

Secret Key

Alice:  1010010

Bob:    1010010
```

- Se mide cuánta *Reconcilied Key* efectiva se tiene en la *Secret Key*:

```
Eficiencia clave secreta:       18.92%
```

- Y cuál sería la eficiencia global comparando con el número de bits de la clave inicial:

```
Eficiencia clave secreta global:        8.75%
```

  - Se comprueba que no se pierden fotones (no hay ningún valor “9” en B1). Es lo esperado al no tener pérdidas en el canal.
  - Se comprueba que el QBER es nulo. Es lo esperado al ser nula la probabilidad de *dark count*.

- Se considera la siguiente configuración del canal (con pérdidas y con efecto de *dark count*, pero sin bits comprometidos):

Parámetro	**Valor**
Longitud de clave a generar (bytes)	10
Pérdidas del canal (%)	20
Probabilidad de *dark count* (‰)	10
Factor de reducción de la *Preliminar Reconcilied Key*	1.15
Nº de bits comprometidos	0

Tabla 2: Configuración propuesta 2 para protocolo *QKD BB84*.

Obteniéndose las siguientes salidas:

- A1, secuencia que representa los bits a codificar en estado cuántico (clave inicial propuesta):

```
A1:     01010100101010010100110100011001011100100111011111100110101011001100100111111101
```

- A2, secuencia que representa la elección de las bases para la codificación cuántica:

```
A2:     01010101100111101101001010101011000011011100100110000001110101001100100000001111
```

- B2, secuencia que representa la elección de las bases para la decodificación cuántica de los qubits recibidos:

```
B2:     01110111011101101100101100110111001011011100111110100100111110101111011110111111
```

Decodifica la cadena de qubits detectada (la mide haciendo uso de las bases B2), dando lugar a la secuencia de bits clásicos:

- B1, secuencia decodificada para obtener A1 (el valor "9" indica "fotón perdido"):

```
B1:     01019100111900010109010100001101091100100191909911091109910101199911001009101001
```

Por tanto, la clave "bruta" (sin procesar) sería:

```
Raw key:        01011001110001010010100001101011001001101101101010111100100101001
Nº coincidencias en las bases:  36 / 80 (45.00%)
```

Alice genera la clave reconciliada preliminar: se queda con los bits de A1 para los que ha coincidido con las bases de Bob:

```
Alice:  01110001010100001010010011111010111101
```

Bob genera la clave reconciliada preliminar: se queda con los bits de B1 para los que ha coincidido con las bases de Alice:

```
Bob:    01110001010100001010010011111010111001
Bits reconciliados:     36 / 80 del total enviado inicialmente
QBER:   1.54%
Reconciled Key (tras el proceso Error Correction)
Alice:  00010101000010100100111110111101
Bob:    00010101000010100100111110111101
Bits reconciliados:     31 / 80 del total enviado inicialmente
```

- Se mide cuánta *Raw Key* efectiva se tiene tras la reconciliación:

```
Eficiencia reconciliación:      47.69%
```

- Y cuál sería la eficiencia global comparando con el número de bits de la clave inicial:

```
Eficiencia reconciliación global:       38.75%
Secret Key
Alice:  1
Bob:    1
```

- Se mide cuánta *Reconcilied Key* efectiva se tiene en la *Secret Key*:

```
Eficiencia clave secreta:       3.23%
```

- Y cuál sería la eficiencia global comparando con el número de bits de la clave inicial:

```
Eficiencia clave secreta global:        1.25%
```

- Se comprueba que se pierden fotones (hay valores “9” en B1). Es lo esperado al considerar pérdidas en el canal.
- Se observa que el QBER no es nulo, y no es extraño que sea así al considerar cierta probabilidad de *dark count*. Pero como esta probabilidad es tan pequeña, en otras ejecuciones con los mismos datos sería lógico que sí diera un resultado nulo.
- Con respecto a los resultados del caso anterior, se observa que la eficiencia de clave secreta es bastante menor, de hecho la longitud de la misma es de

un único bit. Sería lógico establecer un umbral mediante el cual considerar como válida o no la clave secreta en función de su longitud (que al menos cumpla con un número mínimo de bits).

- Se considera la siguiente configuración del canal (con pérdidas y con efecto de *dark count*, y además ciertos bits comprometidos):

Parámetro	**Valor**
Longitud de clave a generar (bytes)	10
Pérdidas del canal (%)	20
Probabilidad de *dark count* (‰)	10
Factor de reducción de la *Preliminar Reconcilied Key*	1.15
Nº de bits comprometidos	3

Tabla 3: Configuración propuesta 3 para protocolo *QKD BB84*.

Obteniéndose las siguientes salidas:

- A1, secuencia que representa los bits a codificar en estado cuántico (clave inicial propuesta):

```
A1:     00111010100000111001110011011001011111011100000100011101001101011100010101110111
```

- A2, secuencia que representa la elección de las bases para la codificación cuántica:

```
A2:     10110111010001001101000010110000000011010110011000100011101111100110010010011101
```

- B2, secuencia que representa la elección de las bases para la decodificación cuántica de los qubits recibidos:

```
B2:     00101111110101111110111010000100000011010010101101100001000010000001111101110111
```

Decodifica la cadena de qubits detectada (la mide haciendo uso de las bases B2), dando lugar a la secuencia de bits clásicos:

- B1, secuencia decodificada para obtener A1 (el valor "9" indica "fotón perdido"):

```
B1:     10101010000900111009009091111001091010000009010909011000010911991900100011191101
```

Por tanto, la clave "bruta" (sin procesar) sería:

```
Raw key:        10101010000001110000011110010101000000010001100001011100100011111101
```

```
Nº coincidencias en las bases:  33 / 80 (41.25%)
```

Alice genera la clave reconciliada preliminar: se queda con los bits de A1 para los que ha coincidido con las bases de Bob:

```
Alice:  01010000010011010110011001010111
```

Bob genera la clave reconciliada preliminar: se queda con los bits de B1 para los que ha coincidido con las bases de Alice:

```
Bob:    01010000010011010110011001010111
```

```
Bits reconciliados:     33 / 80 del total enviado inicialmente
```

```
QBER:   0.00%
```

Reconciled Key (tras el proceso Error Correction)

```
Alice:  00000100110101100110010101111
```

```
Bob:    00000100110101100110010101111
```

```
Bits reconciliados:     29 / 80 del total enviado inicialmente
```

- Se mide cuánta *Raw Key* efectiva se tiene tras la reconciliación:

```
Eficiencia reconciliación:      43.28%
```

- Y cuál sería la eficiencia global comparando con el número de bits de la clave inicial:

```
Eficiencia reconciliación global:       36.25%
```

```
No hay suficiente material para generar la Secret Key
```

- Se comprueba que se pierden fotones (hay valores “9” en B1). Es lo esperado al considerar pérdidas en el canal.
- Se observa que el QBER es nulo, a pesar de considerar cierta probabilidad de *dark count*. Pero como se indicaba en el caso anterior, esta probabilidad es tan pequeña que no es extraño obtener un resultado nulo.
- Con respecto a los resultados del caso anterior, que ya daba un resultado al límite (una clave secreta de tan sólo un bit), ahora al haber añadido también un cierto número de bits comprometidos haciendo que la clave secreta se reduzca más aún, el resultado de la simulación es que no hay suficiente material (bits) para generar una clave secreta.

5.2. Análisis de Canal Cuántico para *QKD BB84*

A continuación se presentan los resultados obtenidos para diferentes configuraciones de los parámetros de entrada, y gráficas comparativas del comportamiento del canal en función de diferentes parámetros.

- Cálculo de pérdidas, QBER y tasa de clave secreta para una configuración manual de parámetros de entrada:

Parámetro	**Valor**
Tipo de configuración	Manual
Ventana óptica (longitud de onda en nm)	2ª (1330)
Diámetro de apertura del transmisor (m)	1
Diámetro de apertura del receptor (m)	1
Atenuación atmosférica (dB/km)	0.1
Longitud total del enlace (km)	300
Longitud del enlace a través de la atmósfera (km)	10
Tiempo de visibilidad diario entre SAT y GS (min)	60
Tipo *BB84*	Clásico
Probabilidad de *dark count* (‰)	0.01
Eficiencia del detector (%)	100
Frecuencia de uso del canal (kHz)	1

Tabla 4: Configuración manual propuesta para análisis del canal cuántico.

Los resultados obtenidos son los siguientes:

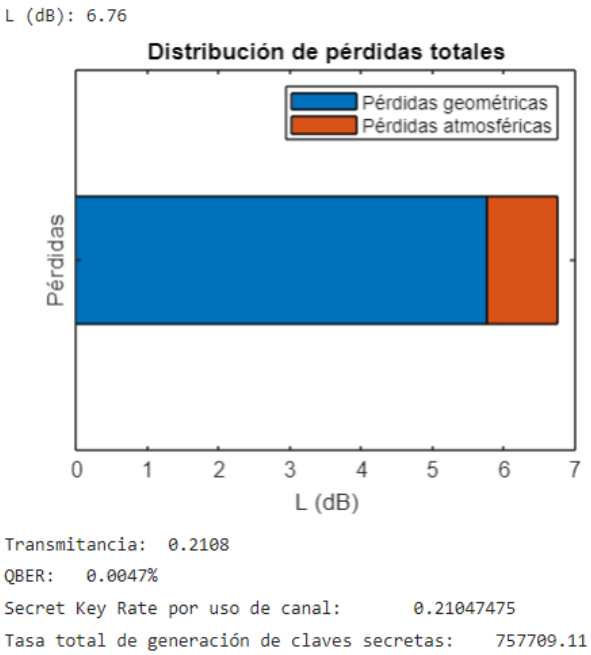

Figura 19: Resultados del análisis para la configuración manual propuesta.

- En cuanto a las pérdidas totales, se observa que la contribución de las pérdidas geométricas o de espacio libre es mayor que las pérdidas atmosféricas (téngase en cuenta que el modelo considerado para el impacto atmosférico es un modelo simple que básicamente considera la absorción por parte de la atmósfera pero no los efectos por turbulencia, que suelen ser de mayor impacto, especialmente en escenarios *uplink*).
- El QBER obtenido tiene un valor pequeño pero no nulo, y es lo esperado al considerar cierta probabilidad de *dark count*. Puede que para algunas configuraciones se muestre un resultado nulo cuando se espera que no lo sea debido al número de cifras decimales consideradas.
- La tasa de clave secreta por uso de canal da lugar a una tasa de generación de claves secretas de más de 7.57e5 (resultado en el que interviene el tiempo total de visibilidad y la frecuencia de uso del canal).

- Gráficas de pérdidas, QBER y tasa de clave secreta en función de diferentes parámetros, considerando para el resto de los parámetros de entrada los definidos en el punto anterior:

  - Representación en función de los parámetros de apertura de emisor y receptor: se observa que a medida que aumenta el diámetro de apertura las pérdidas y el QBER disminuyen, haciendo que la tasa de clave secreta aumente. En esta última se observa además que es más importante disponer de una apertura mayor para el transmisor que para el receptor.

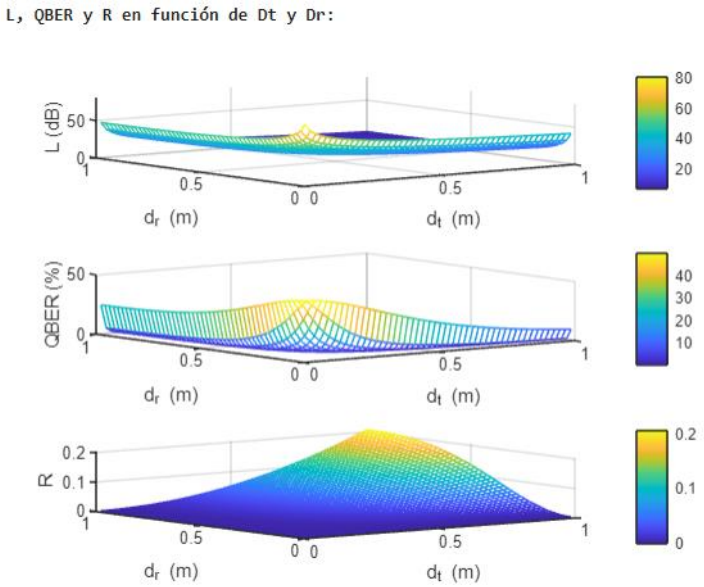

Figura 20: Pérdidas, QBER y tasa de clave secreta en función de los diámetros de apertura de emisor y receptor.

- Representación en función del parámetro de longitud total del enlace: se observa que a medida que aumenta la longitud del enlace también aumentan tanto las pérdidas como el QBER, aunque no de la misma forma, ya que en el caso del QBER este se mantiene muy bajo y es a partir de cierta longitud cuando su valor empieza a aumentar de manera casi exponencial. En cuanto a la tasa de clave secreta, se observa que va disminuyendo conforme aumenta la longitud del enlace, y es a partir de una determinada longitud cuando su valor se mantiene prácticamente nulo.

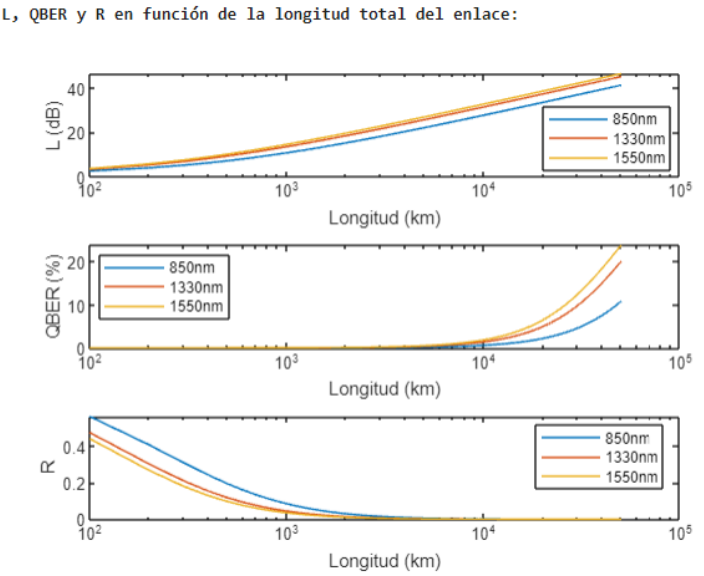

Figura 21: Pérdidas, QBER y tasa de clave secreta en función de la longitud total del enlace.

- Representación en función del parámetro de la distancia que atraviesa el enlace a través de la atmósfera: se observa que a medida que aumenta la longitud del enlace en la atmósfera también aumentan tanto las pérdidas como el QBER, mientras que la tasa de clave secreta disminuye. En este caso las variaciones observadas son bastante lineales.

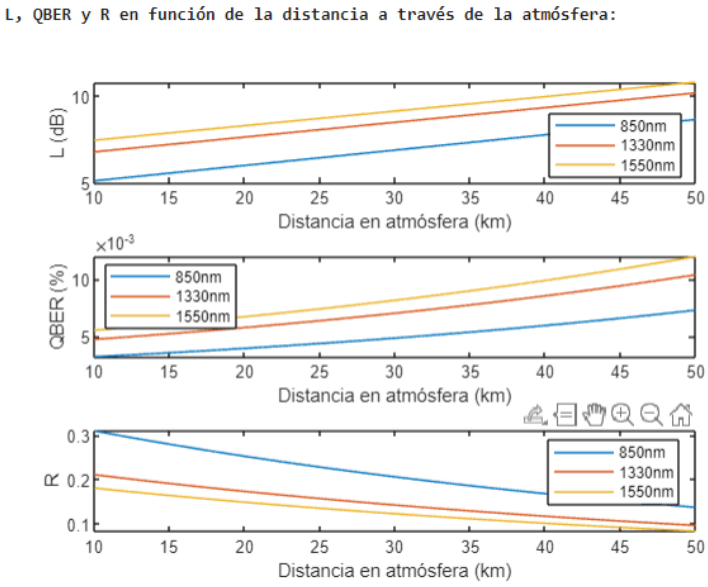

Figura 22: Pérdidas, QBER y tasa de clave secreta en función de la distancia que recorre el enlace a través de la atmósfera.

- Representación en función del parámetro de atenuación atmosférica: se observa que aumenta la atenuación atmosférica (por ejemplo a medida que empeoran las condiciones climáticas) aumentan también las pérdidas de forma lineal. En cuanto al QBER, hay un rango de valores de la atenuación atmosférica en el que este pasa rápidamente de ser prácticamente nulo a llegar a llegar a un valor en el que luego ya se mantiene. Algo similar pasa con la tasa de clave secreta, pero a la inversa, pasando de un valor máximo al nulo en el que se mantiene a partir de cierto valor de atenuación atmosférica.

```
L, QBER y R en función de la atenuación atmosférica:
```

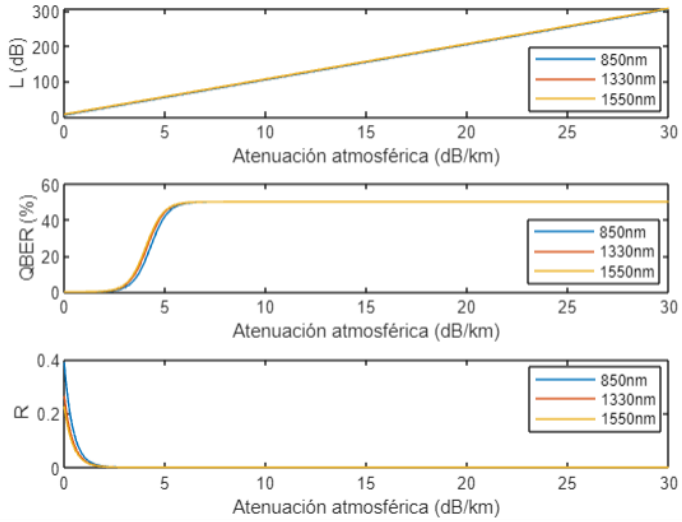

Figura 23: Pérdidas, QBER y tasa de clave secreta en función del parámetro de atenuación atmosférica.

- Representación en función de la probabilidad de *dark count*: en este caso las pérdidas se calculan como valor único, ya que no son dependientes de este parámetro. En cuanto al QBER se observa que este aumenta conforme lo hace la probabilidad de *dark count*, mientras que la tasa de clave secreta se va reduciendo pero es casi inapreciable su variación.

```
L, QBER y R en función de la probabilidad de dark count:
L (dB) para 850nm:      5.09
L (dB) para 1330nm:     6.76
L (dB) para 1550nm:     7.43
```

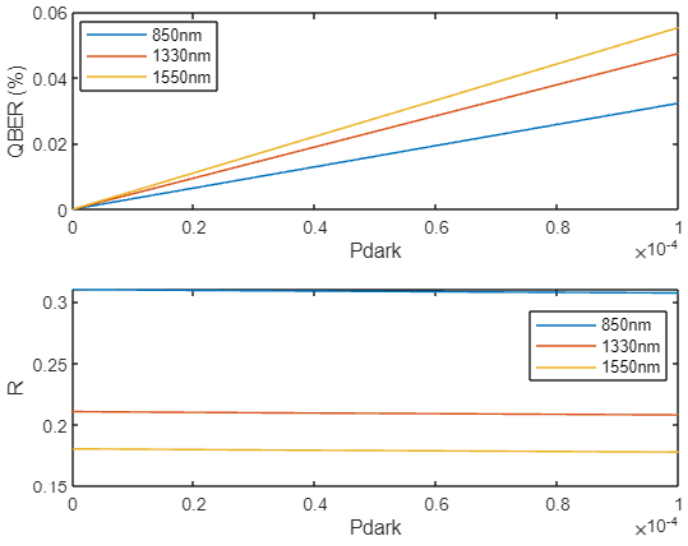

Figura 24: Pérdidas, QBER y tasa de clave secreta en función de la probabilidad de *dark count*.

- Representación en función de la eficiencia del detector: en este caso las pérdidas se calculan de nuevo como valor único, ya que no son dependientes de este parámetro. En cuanto al QBER se observa que este disminuye de forma rápida en cuanto la eficiencia del detector incrementa un poco, y ya luego se mantiene prácticamente nulo. Algo similar ocurre con la tasa de clave secreta pero a la inversa, incrementando de forma rápida en cuanto aumenta un poco la eficiencia del detector y manteniéndose luego prácticamente en el mismo valor.

```
L, QBER y R en función de la eficiencia del detector:
L (dB) para 850nm:      5.09
L (dB) para 1330nm:     6.76
L (dB) para 1550nm:     7.43
```

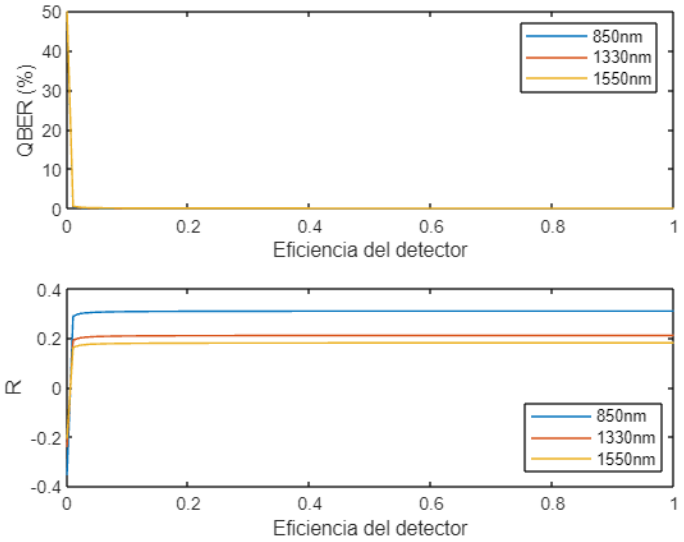

Figura 25: Pérdidas, QBER y tasa de clave secreta en función de la eficiencia del detector.

- Comparativa de la tasa de clave secreta para cada una de las órbitas consideradas en los ficheros TLE.
  Para poder realizar la comparativa hay que elegir una configuración diferente a la manual, lo cual implica que se ignoren algunos parámetros que sólo se utilizan para la configuración manual y haya que definir otros en su lugar:

Parámetro	**Valor**
Tipo de configuración	LEO
Ventana óptica (longitud de onda en nm)	2ª (1330)
Diámetro de apertura del transmisor (m)	1
Diámetro de apertura del receptor (m)	1
Atenuación atmosférica (dB/km)	0.1
Fecha de inicio de la simulación (dd/mm/aaaa)	15/05/2023
Hora de inicio de la simulación (hh:mm)	12:00
Duración de la simulación (días)	7
Latitud GS (º)	40.4168

Longitud GS (º)	-3.7038
Tipo *BB84*	Clásico
Probabilidad de *dark count* (‰)	0
Eficiencia del detector (%)	100
Frecuencia de uso del canal (kHz)	1

Tabla 5: Configuración propuesta para comparativa de tasa de generación de claves entre diferentes órbitas.

El resultado muestra (para los parámetros definidos) que la tasa de generación de claves es mayor para la órbita más baja (LEO) y menor para la órbita más lejana (HEO). Sin embargo, en el caso de la órbita MEO que tiene una altitud algo menor a la GEO, su tasa diaria no es mayor que para la órbita GEO, y esta diferencia es debida al tiempo de visibilidad diario ya que en el caso de la órbita GEO la visibilidad es total (24x7x365) mientras que en el caso de la órbita MEO (o cualquiera de las otras) siempre será menor. De ahí que el resultado sea el mostrado en la siguiente gráfica:

```
Distancia total del enlace (km) para LEO, MEO, GEO, HEO:        1063.86 35544.3 38153.9 43651.7
Tiempo total de visibilidad (min) para LEO, MEO, GEO, HEO:      210 4706 10080 4364
Tasa total de generación de claves secretas para una simulación de 7 días:
```

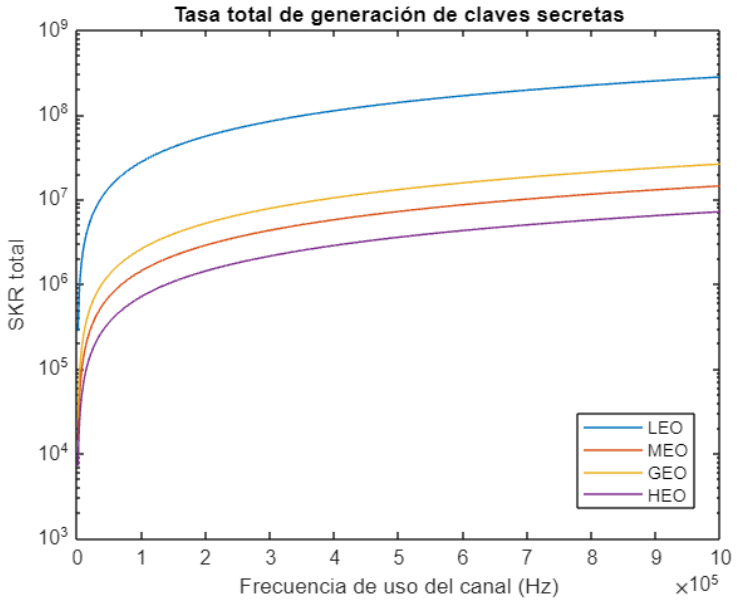

Figura 26: Comparativa de tasa diaria de clave para diferentes órbitas.

6. Conclusiones y trabajos futuros

El objetivo principal de este trabajo ha sido el desarrollo en MATLAB (*LiveScript*) de un simulador para comunicaciones satelitales, dirigido a la comunidad educativa, que permita estudiar tanto el funcionamiento del protocolo *QKD BB84* como el comportamiento del canal de comunicación cuántica en base al marco teórico descrito para dicho canal y protocolo.

Tras el desarrollo de dicho software, se han realizado algunas simulaciones para diferentes configuraciones de los parámetros de entrada, analizando y comparando los resultados obtenidos.
Mediante los resultados obtenidos con las simulaciones realizadas para ver el funcionamiento del protocolo *QKD BB84* se ha podido ver cómo influye la existencia de pérdidas en el canal cuántico sobre la pérdida de fotones que no serán recibidos por el receptor, así como el efecto de *dark count* (detección de fotones inexistentes por parte del receptor) sobre el QBER. También se ha visto cómo además tanto estos parámetros como el factor de reducción y el número de bits comprometidos implican que la clave secreta final sufra una reducción mayor en cuanto a bits, resultando en algunos casos inviable la obtención de una clave secreta por falta de material (bits) para generarla, lo que supondría iniciar de nuevo el protocolo.
En cuanto a los resultados obtenidos con las simulaciones realizadas para ver el comportamiento del canal cuántico para el uso del protocolo *QKD BB84*, se ha podido ver cómo influye cada uno de los parámetros en los resultados obtenidos para las pérdidas, QBER, tasa de clave secreta por uso de canal y tasa de clave secreta para un determinado periodo de tiempo, comprobando que siguen la evolución esperada según las expresiones del modelo teórico utilizado para dicho canal. Así mismo, también se ha visto cómo influye tanto la longitud del enlace como el tiempo de visibilidad en el resultado de tasa de clave secreta (dado un periodo de tiempo) para diferentes órbitas.

En cuanto a trabajos futuros, se han identificado durante la realización del trabajo varias líneas de trabajo:

- Estimación de QBER en el protocolo *QKD BB84*: analizar los algoritmos existentes para llevar a cabo esta estimación e implementarlo en *QKD_BB84_Protocol.mlx*, sustituyendo el cálculo que se realiza con el código actual tomando ventaja de que se trata de una simulación, de manera que en lugar de un cálculo se realice una estimación, que es como funcionaría realmente el protocolo.

- Considerar un posible intruso en el protocolo *QKD BB84*: añadir al funcionamiento simulado del protocolo el caso de que pudiera haber presente un posible intruso, bien de forma simplificada siendo el usuario el que indique si lo hay o no, o bien detectando si la comunicación pudiera estar comprometida utilizando las métricas necesarias analizando el marco teórico necesario.

- Proceso de corrección de errores del protocolo *QKD BB84*: analizar los algoritmos existentes para llevar a cabo este proceso y añadir su implementación en *QKD_BB84_Protocol.mlx*, sustituyendo la corrección de errores simplificada que se ha realizado en este trabajo (aprovechando que se trataba de una simulación) por un algoritmo que represente el proceso de forma más real.

- Proceso de amplificación de privacidad del protocolo *QKD BB84*: al igual que con el proceso de corrección de errores, analizar los algoritmos existentes para llevar a cabo el proceso y sustituir el utilizado en *QKD_BB84_Protocol.mlx*.

- Modelado de pérdidas del canal cuántico: analizar los diferentes modelos de pérdidas para el canal cuántico y sustituir el existente en *QKD_BB84_QChannel.mlx* (que es simplificado) por uno que tenga en cuenta más efectos. El cambio habría que aplicarlo también sobre la función *lossesQuantumChannel.m*.

- Tiempo de visibilidad: añadir al código existente la diferenciación entre visibilidad diurna y nocturna, de forma que sólo se consideren los intervalos de visibilidad nocturna como útiles para *QKD*, ignorando los diurnos.

- Opciones de órbitas: añadir más opciones de órbitas en *QKD_BB84_QChannel.mlx* mediante diferentes ficheros TLE (por ejemplo varios ficheros TLE de diferentes satélites de una misma órbita). Aunque los ficheros TLE utilizados son reales, estos no son genéricos sino que corresponden a satélites concretos, por lo que pueden incluirse otros para analizar casos de diferentes satélites y comparar los resultados entre ellos.

De forma más general, otros trabajos futuros para completar el simulador serían el desarrollo de un código similar pero para otros protocolos *QKD* (por ejemplo E92 o EPR), llegando a integrarlo todo en un único interfaz de usuario para comparar los resultados entre protocolos, y el análisis concreto de los diferentes tipos de comunicación cuántica (enlace ascendente, enlace descendente, y enlace intersatelital).

En cuanto a la consecución de los objetivos, se considera que se han alcanzado todos los planteados inicialmente, pero cabe mencionar que en cuanto a las prestaciones del canal de comunicación no se ha llegado a analizar el funcionamiento de *QKD* en relación con el canal de comunicación clásico en satélite (radiofrecuencia).

Por otra parte, aunque en líneas generales se ha seguido la planificación y metodología prevista, ha sido necesario introducir algunos cambios para garantizar el éxito del trabajo. Inicialmente se había planteado un simulador que contemplase los tres protocolos *QKD* del trabajo de referencia [1], considerando que podría reutilizarse el código de dicho trabajo para esos protocolos sin necesidad de introducir muchos cambios. Pero al analizar detenidamente el código desarrollado en dicho trabajo se vio que era no describía con el detalle o de la forma deseada el funcionamiento del primer protocolo (*BB84*), de manera que aunque sí se ha utilizado como punto de partida, prácticamente se ha rehecho el código teniendo en cuenta los efectos que se querían considerar según el modelo planteado y se ha detallado el funcionamiento del mismo con una simulación más ajustada a la realidad, dando lugar a que hayan quedado fuera del simulador los otros protocolos y por ello se planteen como líneas de trabajo futuro.

7. Glosario

ISL, Inter-Satellite Link
QBER, Quantum Bit Error Rate
QKD, Quantum Key Distribution
Qubit, Quantum bit
SKR, Secret Key Rate

8. Bibliografía

[1] A. V. Marin, *Trabajo final de grado: Simulación y análisis de sisstemas de distribución de clave cuántica,* UPC, 2018.

[2] N. Gisin y R. Thew, «Quantum Communication,» *Nature Photonics,* vol. 1, nº 3, pp. 165-171, 2007.

[3] CSA QUCATS, «Quantum Flagship,» Noviembre 2022. [En línea]. Available: https://qt.eu/app/uploads/2022/11/Quantum-Flagship_SRIA_2022.pdf. [Último acceso: Marzo 2023].

[4] Doctorats Industrials, «DISTRIBUCIÓN CUÁNTICA DE CLAVES CRIPTOGRÁFICAS PARA LARGAS DISTANCIAS DE COMUNICACIÓN,» [En línea]. Available: https://doctoratsindustrials.gencat.cat/es/doctorats/distribucion-cuantica-de-claves-criptograficas-para-largas-distancias-de-comunicacion/. [Último acceso: Marzo 2023].

[5] A. Aji, K. Kurunandan y P. Krishnan, «A Survey of Quantum Key Distribution (QKD) Network,» de *2021 2nd Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, 2021.

[6] L. O. MAILLOUX, D. D. HODSON, M. R. GRIMAILA, R. D. ENGLE, C. V. MCLAUGHLIN y G. B. BAUMGARTNER, «Using Modeling and Simulation to Study Photon Number Splitting Attacks,» *IEEE Access,* vol. 4, pp. 2188-2197, 2016.

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus y M. Peev, «The security of practical quantum key distribution,» *Reviews of Modern Physics,* vol. 81, nº 3, pp. 1301-1350, 2009.

[8] A. Carrasco-Casado y R. Mata-Calvo, «Space Optical Links for Communication Networks,» de *Springer Handbook of Optical Networks*, Springer Handbooks, 2020, pp. 1057-1103.

[9] A. G. Alkholidi y K. S. Altowij, «Free Space Optical Communications — Theory and Practices,» de *Contemporary Issues in Wireless Communications*, IntechOpen, 2014, pp. 159-212.

[10] C. Zhang, A. Tello, U. Zanforlin, G. S. Buller y R. J. Donaldson, «Link loss analysis for a satellite quantum communication down-link,» *Proceedings of SPIE,* vol. 11540, 2020.

[11] AcademiaLab, «Distribución de claves cuánticas,» [En línea]. Available: https://academia-lab.com/enciclopedia/distribucion-de-claves-cuanticas/. [Último acceso: Marzo 2023].

[12] R. Bedington, J. M. Arrazola y A. Ling, «Progress in satellite quantum key distribution,» *Nature,* vol. 3, nº 30, 2017.

[13] J. Wang y B. A. Huberman, «An Overview on Deployment Strategies for Global Quantum Key Distribution Networks,» *Wireless Communications and Mobile Computing,* vol. 2022, nº 9927255, pp. 1-15, 2022.

[14] C. Caputo, M. Simoni, G. A. Cirillo, G. Turvani y M. Zamboni, «A simulator of optical coherent-state evolution in quantum,» *Springer,* vol. 54, nº 689, 2022.

[15] A. A. G. Calle, *Proyecto final de carrera: Diseño de un simulador de comunicaciones por satélite y posterior estudio de prestaciones para diferentes configuraciones,* UPC, 2014.

[16] À. Barberà y J. I. Morales Volosín, «Lanzamientos Espaciales,» [En línea]. Available: https://lanzamientosespaciales.com/tipos-orbitas/. [Último acceso: 15 05 2023].

[17] H. Riebeek, «Earth Observatory - NASA,» [En línea]. Available: https://earthobservatory.nasa.gov/features/OrbitsCatalog#:~:text=There%20are%20essentially%20three%20types,farthest%20away%20from%20the%20surface. [Último acceso: 15 05 2023].

[18] Federal Aviation Administration, «Federal Aviation Administration,» [En línea]. Available: https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/aam/cami/library/online_libraries/aerospace_medicine/tutorial/media/iii.4.1.4_describing_orbits.pdf. [Último acceso: 15 05 2023].

[19] C. Liorni, H. Kampermann y D. Bruß, «Satellite-based links for quantum key distribution: beam effects and weather dependence,» *New Journal of Physics,* vol. 21, nº 093055, 2019.

[20] Q. Chen, L. Yang, X. Liu, B. Cheng, J. Guo y X. Li, «Modeling and Analysis of Inter-Satellite Link in LEO Satellite Networks,» *IEEE: 13th International Conference on Communication Software and Networks (ICCSN),* nº 10.1109/ICCSN52437.2021.9463648, pp. 134 - 138, 2021.

[21] S. DiAdamo, B. Qi, G. Miller, R. Kompella y A. Shabani, «Packet Switching in Quantum Networks: A Path to Quantum Internet,» *Quantum Physics,* nº arXiv:2205.07507, p. 14, 2022.

[22] C. Gobby, Z. L. Yuan y A. J. Shields, «Quantum key distribution over 122 km of standard telecom fiber,» *Applied Physics Letters,* vol. 84, nº 19, pp. 3762-3764, 2004.

[23] H. Shu, «Asymptotically Optimal Quantum Key Distribution Protocols,» *Quantum Physics,* nº arXiv:2110.01973, 2022.

[24] Orbiting Now, «Orbiting Now,» [En línea]. Available: https://orbit.ing-now.com/. [Último acceso: 15 04 2023].

[25] RF Wireless World, «RF Wireless World,» [En línea]. Available: https://www.rfwireless-world.com/calculators/satellite-slant-range-calculator.html. [Último acceso: 3 Junio 2023].

9. Anexos

9.1. Anexo I: Fases del protocolo *BB84*

1. Alice genera una secuencia aleatoria de ceros y unos $A_1 = a_1, a_2, \dots, a_N$, con $a_k \in \{0, 1\}$. Supongamos que por ejemplo $A_1 = 0, 0, 1, 1$.

2. Para cada bit de la cadena A_1, Alice elige aleatoriamente entre dos bases (Z, X), con $Z = \{|0\rangle, |1\rangle\}$ y $X = \{|+\rangle, |-\rangle\}$. Supongamos que esta elección se traduce en otra secuencia aleatoria (secuencia de bases) donde un cero indica que se utiliza la base Z y un uno indica que se utiliza la base X, dando lugar a una secuencia $A_2 = a'_1, a'_2, \dots, a'_N$, con $a'_k \in \{0, 1\}$. Supongamos que por ejemplo $A_2 = 0, 1, 0, 1$.

3. Alice envía la secuencia de bits A_1 codificada con la base correspondiente, dada por la cadena A_2. Es decir, mediante el canal cuántico Alice envía una secuencia de qubits, que para el ejemplo considerado sería $A = |0\rangle, |+\rangle, |1\rangle, |-\rangle$.

4. Bob recibe la secuencia de qubits A, y para medirla elige de forma aleatoria la base con la que hacerlo. Para ello genera una secuencia aleatoria de bits $B_2 = b'_1, b'_2, \dots, b_{,N}$, con $b'_k \in \{0, 1\}$, donde al igual que en el punto 2 el cero indica que se utiliza la base Z y el uno indica que se utiliza la base X. Supongamos que por ejemplo $B_2 = 1, 0, 0, 1$.

5. Bob realiza la medida de la secuencia A en base a su elección de bases B_2. Si la base elegida para la medida de cada qubit coincide con la que había utilizado Alice para la codificación, entonces el valor medido (0 ó 1) tiene un 100% de probabilidad, mientras que si la base para la medida no coincide con la que había utilizado Alice el valor medido (0 ó 1) tiene un 50% de probabilidad. Para el caso de ejemplo propuesto, Bob estaría midiendo los dos primeros qubits con una base diferente a la que usó Alice para codificar, y los dos segundos qubits con la misma base que usó Alice, por lo que la secuencia medida por Bob sería $0/1, 0/1, 1, 1$ (donde 0/1 indica que puede tenerse un 0 ó 1 con probabilidad del 50%). Supongamos que la secuencia medida hubiera resultado en $B_1 = 1, 0, 1, 1$.

6. Alice envía a Bob la secuencia A_2 por el canal clásico ($A_2 = 0, 1, 0, 1$) y Bob responde con las posiciones donde $B_2 = A_2$, que para el caso del ejemplo serían las posiciones 3ª y 4ª. Si el número de posiciones enviadas por Bob es menor que dos, la sesión debe abortarse y reiniciarse con nuevas secuencias aleatorias (puede establecerse el umbral de error que se requiera).

7. Alice se quedará con aquellos bits de la secuencia A_2 que correspondan con las posiciones que Bob le ha indicado, generando una *reconciled key*, $A_{reconciled-key}$. Para el ejemplo se tendría que $A_{reconciled-key} = 0,1$. Y Bob, a partir de la secuencia B_2 y las posiciones que ha enviado a Alice para las que $B_2 = A_2$, genera su propia *reconciled key*, $B_{reconciled-key}$. En el ejemplo, $B_{reconciled-key} = 0,1$.

8. Alice y Bob generan una nueva clave, una *secret key*, con un mayor nivel de seguridad (ampliación de privacidad) a partir de la *reconciled key*. Si para esto se opta por usar el operador lógico XOR, para ejemplificar de forma sencilla el proceso, entonces el cálculo de los bits restantes para la secuencia (hasta llegar a N) se calcula como $a_3'' = a_1'' \oplus a_2''$, $a_4'' = a_2'' \oplus a_3''$ y $b_3'' = b_1'' \oplus b_2''$, $b_4'' = b_2'' \oplus b_3''$. Para el ejemplo: $a_3'' = 0 \oplus 1 = 1$, $a_4'' = 1 \oplus 1 = 0$, $b_3'' = 0 \oplus 1 = 1$, $b_4'' = 1 \oplus 1 = 0$, y por tanto $A_{secret-key} = B_{secret-key} = 0,1,1,0$.

9.2. Anexo II: Cálculo del rango de un satélite

Para obtener la distancia del enlace GS-SAT a través de la atmósfera se ha utilizado el mismo cálculo que para el rango de un satélite, considerando en este caso que la altitud corresponde con la de la atmósfera, dando lugar a la expresión [25]:

$$D\ (km) = \sqrt{(R \cdot \cos(\epsilon))^2 + (R+h)^2 - R^2} - R \cdot \cos\ (\epsilon)$$

Donde $R\ (km)$ es el radio terrestre, $h\ (km)$ es la altura de la atmósfera (se ha considerado un valor de 10 km) y $\epsilon = 90 - \alpha$ (°) es el ángulo de elevación de la estación terrena.

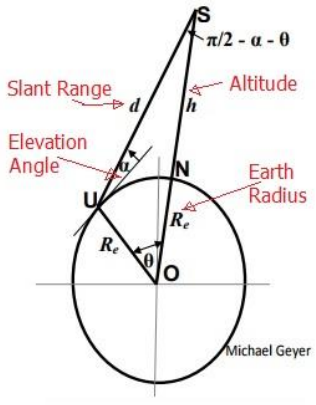

Figura 27: Cálculo del rango de un satélite.