Trabajo Integrador
Control Remoto

Elías Courdin
Comunicaciones Digitales 2025
Facultad de Ingeniería
Montevideo, Uruguay
eliascourdin15@gmail.com

Uriel Yaffé
Comunicaciones Digitales 2025
Facultad de Ingenieria
Montevideo, Uruguay
urielyaffe@gmail.com

Fig. 1. [4] Puerta de Garage con Receptor

I. Introducción a la tecnología

La tecnología de comunicación que se que se estudia en este trabajo es la utilizada en los controles remotos, específicamente en los controles para portones eléctricos. Estos sistemas son ampliamente utilizados en viviendas, edificios y garajes, tanto para facilitar el acceso vehicular automatizado como para aportar en materia de seguridad, eficiencia y comodidad.

Un sistema típico de apertura de portón eléctrico se puede observar en la figura 1. Consta principalmente de un control remoto, que oficia de transmisor móvil, y un receptor fijo directamente conectado con el funcionamiento mecánico del portón. Al presionar un botón en el control remoto, este transmite una señal de radiofrecuencia codificada al receptor ubicado en el portón. Cuando el receptor recibe la señal y detecta que es válida, se activa un motor eléctrico que abre o cierra la puerta según corresponda.

A lo largo del tiempo, la tecnología de estos dispositivos ha evolucionado. Los modelos más antiguos utilizaban códigos fijos, definidos por interruptores (DIP switches) que permitían que dos controles diferentes enviaran señales idénticas si estaban configurados con el mismo código. Esto dio origen al problema ”open-the-neighbor-gate”, donde un control remoto podía accionar accidentalmente o intencionalmente el portón de otra vivienda cercana que usara el mismo código.
Este problema comenzó a resolverse con el aumento en la cantidad de DIP switches en los controles remotos, lo que permitió generar una mayor cantidad de combinaciones de códigos fijos, mitigando en gran medida el problema anterior. Sin embargo, en los últimos tiempos surgieron problemas de seguridad vinculados a ataques de ”replay”, ya que aunque los códigos fueran diferentes aún eran fijos. Cualquier atacante capaz de recibir el código que emite un control y transmitirlo, puede violar la seguridad del sistema. Este problema de seguridad se discute más adelante junto con un sistema de códigos que logra solucionar esta problemática.

II. Objetivos

Este trabajo tiene como objetivo principal el estudio del sistema de comunicación transmisor-receptor utilizado en controles remotos para portones eléctricos. Se analizarán las señales involucradas en la transmisión, su modulación y el proceso correspondiente de demodulación por parte del receptor.
Asimismo, se busca discutir distintos aspectos relacionados con el diseño del sistema, tales como su eficiencia, simplicidad, y especialmente su seguridad frente a ataques externos.
Como parte del trabajo práctico, se realizaron experimentos orientados a evaluar la vulnerabilidad de sistemas basados en código fijo, mediante ataques de repetición (replay attacks) utilizando un dispositivo HackRF One. Además, se analizaron señales de controles remotos más avanzados que emplean codificación Rolling Code, comparando su robustez frente a este tipo de ataques.

III. Modulación

Los controles remotos habituales para portones eléctricos transmiten un código binario por radiofrecuencia, comunmente en la banda de los 433MHZ.
La comunicación se realiza mediante el envió de un código fijo, esto quiere decir que el mensaje enviado por el emisor es siempre la misma tira de bits.

A. ASK

La modulación más comunmente utilizada por estos dispositivos es la denominada ASK (Amplitude Shift Keying). La modulación por desplazamiento de amplitud (ASK), es una forma de modulación en la cual se representan los datos digitales como variaciones de amplitud de la onda portadora en función de los datos a enviar [1] que es análoga a la modulación vista en el curso BPSK, pero se modula en

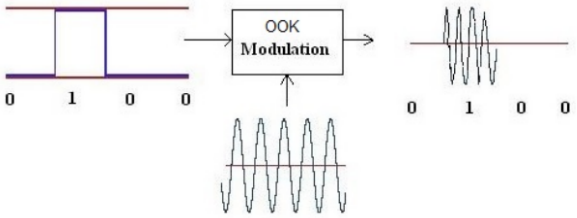

Fig. 2. [3] Modulación OOK

amplitud y no en fase. La forma que toma la señal en el tiempo se puede escribir como:

$$Y_{ASK}(t) = A(t) \times sen(2\pi ft + \phi)$$

Donde cada símbolo "i" es representado por una amplitud $A(t) = A_i$ diferente. En particular, los controles remotos utilizan el tipo mas sencillo de modulación ASK binaria, llamada OOK (On-Off Keying).

B. OOK

1) Aspectos generales: On-Off Keying consiste simplemente en encender o apagar la portadora según el bit que se quiere enviar, es decir, usar $A(t) = 0$ para enviar un "0" y un valor de amplitud no nulo para enviar "1", así como se observa en la figura 2. Este funcionamiento es similar a como se puede usar una linterna para enviar un código morse, encendiendo y apagando la luz.

La modulación OOK destaca por una serie de ventajas. En primer lugar, al transmitir señal únicamente para uno de los símbolos, resulta bastante eficiente en términos energéticos, lo que la hace especialmente adecuada para dispositivos portátiles alimentados por batería. Otra ventaja destacable es su simplicidad tanto en la implementación como en la demodulación, motivo por el cual se emplea con frecuencia en sistemas de comunicación de bajo costo.

Sin embargo, una de las principales desventajas de OOK es su elevada sensibilidad al ruido electromagnético. Dado que la información se codifica en la amplitud de la señal, cualquier perturbación en el entorno que afecte esta magnitud puede comprometer la integridad de la transmisión.

En cuanto a la sicronización entre emisor y receptor, normalmente en controles remoto no existe un mecanismo tal como relojes, sino que normalmente se envía al inicio del código un preambulo conocido, como puede ser "1010", que el receptor usa para identificar el tiempo de símbolo que utiliza el emisor y de esa forma sicronizarse.

Un ejemplo de transmisión de bits utilizando modulación OOK puede observarse en la Figura 3. La señal fue capturada utilizando un dispositivo HackRF One, en el marco de un experimento informal realizado por Paul Rascagnères, documentado en [5], y visualizada mediante la herramienta GNU Radio.

En la figura 4 se muestran los bits identificados en la señal de la figura 3.

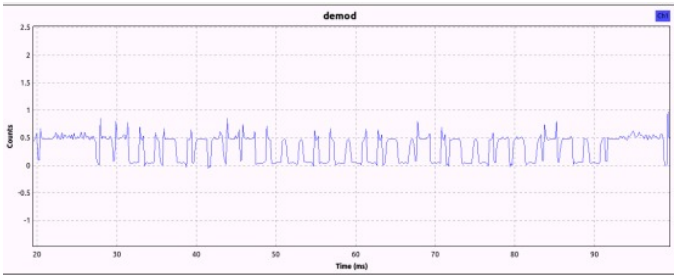

Fig. 3. Señal modulada en OOK visualizada en GNU Radio

Fig. 4. Identificación de bits en la señal OOK

Este tipo de sistemas de comunicación, al ser tan simples, no incorporan mecanismos de corrección de errores, incluso siendo sensibles al ruido. Una estrategia común para aumentar la robustez frente a errores de transmisión, como se observa en el experimento documentado en [5], consiste en repetir varias veces el mismo código cada vez que se presiona el botón, de modo que el receptor tenga más oportunidades de decodificar correctamente el mensaje, incluso en presencia de interferencias.

2) Aspectos específicos: La constelación de una modulación OOK se muestra en la Figura 6, donde el umbral V_T se ubica en la mediatriz entre ambos símbolos.

La energía del símbolo es $E_S = \sum_{i \in \{0,1\}} \text{prob}_i \cdot E_i$, donde cada $E_i = \int |p_i(t)|^2 dt$.

Como para mandar un '0' no se transmite pulso, $p_0(t) = 0$, por lo tanto $E_0 = 0$, y queda:

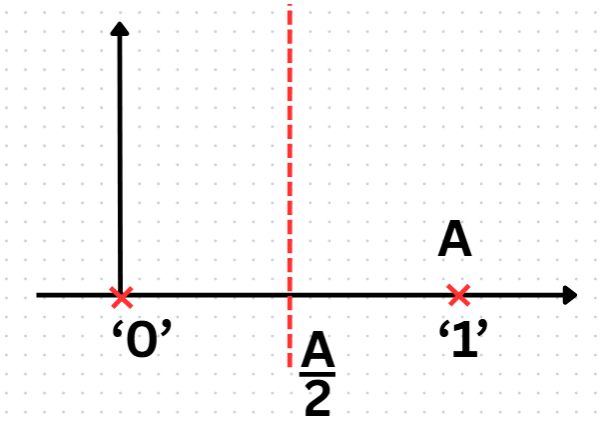

Fig. 5. Constelación OOK

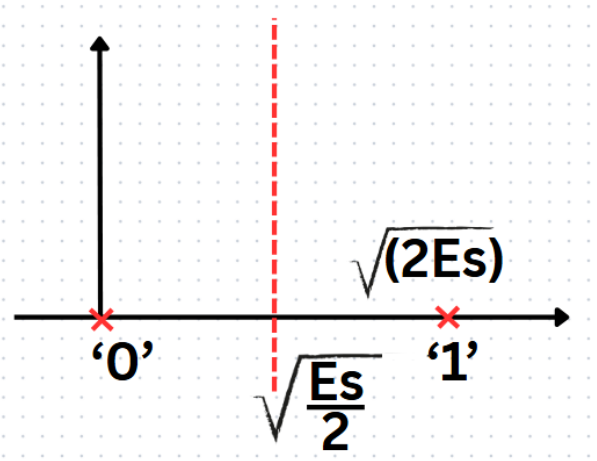

Fig. 6. Constelacion OOK

$$E_S = \text{prob}_1 \cdot E_1 = \text{prob}_1 \cdot \int |p_1(t)|^2 dt = \text{prob}_1 \cdot A^2 \cdot \|p\|^2$$

Asumiendo pulsos normalizados y bits equiprobables:

$$E_S = \frac{A^2}{2} \longrightarrow A = \sqrt{2E_S}$$

Para calcular la probabilidad de error:

$$P_{eb} = P_{e0} \cdot \text{prob}_0 + P_{e1} \cdot \text{prob}_1$$

Asumiendo que el ruido es gaussiano, para que se genere un error el ruido debe llevar la señal al otro lado del umbral. Para esto se calcula:

$$P_{e0} = P(Y > V_T \mid Y_D \sim \mathcal{N}(0, \sigma^2)) = P(N_D > V_T)$$

$$P_{e1} = P(Y_D < V_T \mid Y_D \sim \mathcal{N}(A, \sigma^2)) = P(A + N_D < V_T)$$

Con $V_T = \frac{A}{2}$, se tiene:

$$P_{e0} = P(N_D > \frac{A}{2}), \quad P_{e1} = P(N_D < -\frac{A}{2})$$

Por simetría de la cola gaussiana:

$$P_{e0} = P_{e1} = Q\left(\frac{A}{2\sigma}\right)$$

$$\Rightarrow P_{eb} = Q\left(\frac{A}{2\sigma}\right)$$

IV. Problemáticas del sistema de comunicación

Un problema que presenta esta tecnología es que, al utilizar una modulación muy sensible al ruido como OOK (On-Off Keying), la comunicación entre el control remoto y el receptor de la puerta funciona de manera confiable solo a distancias relativamente cortas.

Por otra parte, la principal problemática de este mecanismo radica en su seguridad. Muchas investigaciones relacionadas con este tema han demostrado que es posible interceptar con facilidad el código enviado por un control, extraer la cadena de bits y reenviarla por radiofrecuencia en la misma banda utilizada por el control. Al hacer esto, el receptor no distingue entre las distintas fuentes y acciona la puerta.

Además, como el código es fijo, una vez obtenida la clave, se podría vulnerar la seguridad cuantas veces se quiera mediante ataques de repetición (Replay Attacks).

Sin embargo, también se han encontrado investigaciones que presentan un nuevo sistema de codificación, ya implementado en otros sistemas de control remoto, denominado *Rolling Code* [8].

V. Rolling Code

El *Rolling Code* es un sistema de autenticación que emplea técnicas criptográficas para proteger las comunicaciones frente a ataques por repetición, un problema común en sistemas con códigos fijos.

Cada vez que se presiona un botón del control remoto, se genera un nuevo código basado en un contador interno que se incrementa, un identificador único del dispositivo e información adicional como puede ser una señalización del botón presionado (por ejemplo, abrir o cerrar). Esta información se cifra utilizando una clave secreta previamente compartida entre el control remoto y el receptor.

Cuando el receptor recibe un mensaje, lo descifra y verifica que el identificador coincida con uno registrado, y que el valor del contador se encuentre dentro de una ventana de validez (*validity window*), es decir, un rango aceptable en torno al último valor recibido. Si ambas condiciones se cumplen, la puerta se abre.

Este funcionamiento implica que cuando un código arbitario que es enviado llega al receptor, deja de ser un código válido en el instante en que el receptor mueve la ventana de validez (actualizando el contador interno)

Gracias a este funcionamiento, el código transmitido cambia en cada uso, lo que lo hace mucho más robusto frente a intentos de clonación o repetición, y resuelve el problema de seguridad presente en los controles con código fijo.

En la figura 7 se observa un ejemplo básico de trama para un código fijo, donde se pueden observar campos de preambulo, y campos de chequeo de errores como *CheckSum*. En la figura 8 se puede observar un esquema básico para entender el funcionamiento del rolling code, muy utilizado en llaves de

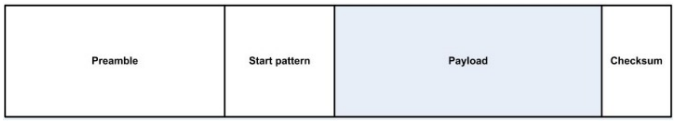

Fig. 7. Ejemplo de trama Rolling Code, extraído de [2]

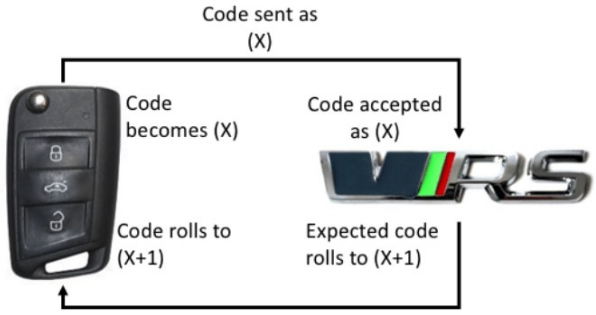

Fig. 8. Esquema de funcionamiento básico del Rolling Code para llaves de autos, extraído de [8]

autos.

A. Cifrado KeeLoq

Normalmente los fabricantes de sistemas de apertura de puertas de garaje no desarrollan sus propios algoritmos de rolling code, sino que adoptan soluciones provistas por empresas especializadas. Un ejemplo destacado es el sistema de código variable desarrollado por Microchip, basado en el cifrado KeeLoq [4], el cual se utiliza ampliamente tanto en sistemas de apertura remota de puertas de garage con control remoto.
Una trama de Rolling Code con cifrado de tipo KeeLoq se observa en la figura 9.

El cifrado KeeLoq es un algoritmo de cifrado propietario ampliamente utilizado en sistemas de control remoto de acceso sin llave (Remote Keyless Entry, RKE), tales como inmovilizadores de automóviles, alarmas, y sistemas de apertura de portones y garajes. Su diseño está orientado a la eficiencia en hardware, lo que lo hace particularmente adecuado para dispositivos embebidos de bajo consumo y bajo costo.

KeeLoq es un cifrado de bloque que opera sobre bloques de 32 bits de texto plano y utiliza una clave de 64 bits. Su núcleo criptográfico está basado en un registro de desplazamiento con realimentación no lineal (NLFSR). El algoritmo realiza 528

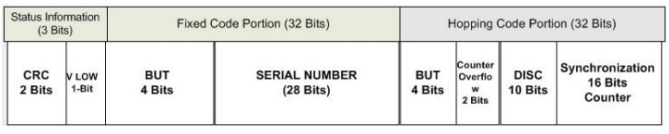

Fig. 9. Ejemplo de trama de Rolling Code del tipo KeeLoq extraído de [3]

ciclos de cifrado, durante los cuales se actualizan los registros internos y se mezcla progresivamente la clave con el texto plano.

B. Problema de seguridad en Rolling Code

A pesar de que los sistemas basados en rolling codes representan una mejora significativa en términos de seguridad frente a ataques de repetición, existen técnicas que permiten vulnerarlos de forma relativamente sencilla. Una de ellas es el denominado ataque RollJam. Este ataque aprovecha una debilidad inherente a muchos receptores: el hecho de que un código solo se marca como utilizado si es efectivamente recibido y validado. El procedimiento consiste en interceptar la señal emitida por el control remoto del usuario cuando este intenta abrir el portón. Simultáneamente, el atacante transmite una señal de interferencia (jamming) que impide que el receptor del portón reciba correctamente dicho código. Como consecuencia, el portón no lo reconoce como usado, pero el atacante logra capturarlo. Repitiendo esta operación en dos ocasiones, el atacante obtiene dos códigos válidos: uno puede utilizarse de inmediato para abrir el portón sin levantar sospechas, mientras que el otro queda almacenado para un acceso no autorizado en el futuro. Este tipo de ataque requiere que el sistema sea vulnerable a interferencias de RF, que el receptor marque como válidos únicamente los códigos que logra recibir, y que la banda de frecuencia utilizada sea lo suficientemente amplia como para permitir tanto la interferencia como la captura de la señal transmitida.

VI. HackRF One

HackRF One es un dispositivo de radio definida por software (SDR) desarrollado por Great Scott Gadgets que permite la transmisión y recepción de señales de radio en un amplio rango de frecuencias, desde 1 MHz hasta 6 GHz. Fue diseñado como una plataforma de hardware de código abierto, con el propósito es facilitar el desarrollo y testeo de tecnologías de comunicación modernas y emergentes. Puede utilizarse como un periférico USB conectado a una computadora, o bien programarse para operar de manera autónoma.
Este dispositivo es compatible con programas ampliamente utilizados como GNU Radio, URH (Universal Radio Hacker), y otros. La página oficial con información y tutoriales se encuentra en [6].

VII. Universal Radio Hacking (URH)

Universal Radio Hacker (URH) es un software desarrollado para la investigación de protocolos inalámbricos, con soporte nativo para muchos dispositivos de radio definidos por software (Software Defined Radios, SDR) tales como HackRF One. URH permite una demodulación sencilla de señales y ofrece detección automática de parámetros de modulación, facilitando la identificación de los bits y bytes que se transmiten por el aire.

Dado que los datos suelen estar codificados antes de ser transmitidos, URH incluye herramientas de decodificación

personalizables que permiten descifrar incluso codificaciones complejas.

Para la ingeniería inversa de protocolos, URH proporciona dos enfoques: por un lado, se pueden asignar manualmente los campos del protocolo y los tipos de mensajes; por otro, URH puede inferir automáticamente estos elementos mediante un sistema de reglas basado en inteligencia heurística.

Finalmente, la herramienta también incorpora un componente de fuzzing para probar la robustez de protocolos sin estado, así como un entorno de simulación para llevar a cabo ataques sobre protocolos con estado.

VIII. Experiencia práctica usando HackRF One

A. Demodulación

Para comenzar con la demodulación, se empezó buscando la frecuencia de la señal transmitida por el control remoto de un portón y de un auto.

Se utilizó la herramienta de software GQRX para obtener un espectrograma en frecuencia de las señales capturadas por el HackRF.

Al presionar el botón del control remoto del portón, se genera un pulso en la frecuencia 436 MHz, donde previamente no se observaba actividad, lo que sugiere que dicha frecuencia es utilizada por el control remoto. Esto se muestra en la Figura 10.

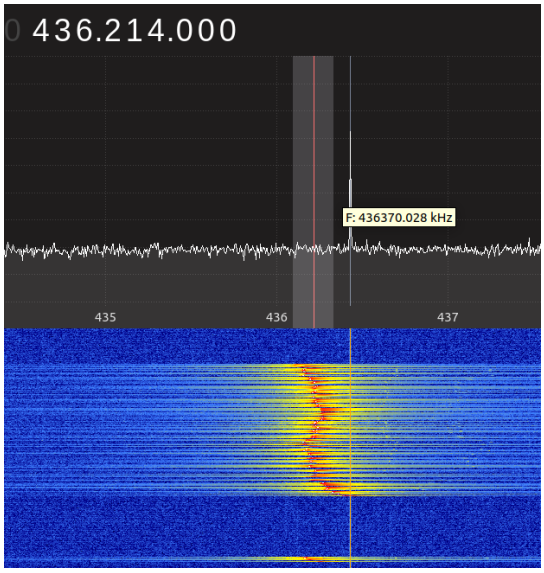

Fig. 10. Espectrograma de la onda recibida de un control remoto de portón

Por otro lado, la señal del control remoto del auto tiene una frecuencia central levemente diferente, está centrada en 434MHz. Se puede ver la comparativa de ambos espectros en la Figura 11.

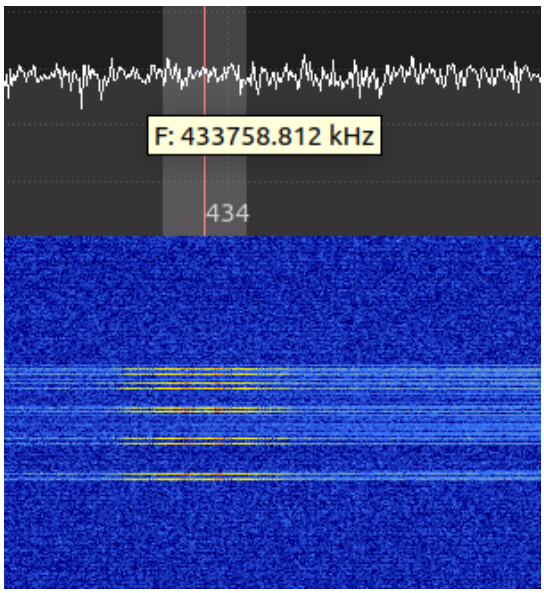

Fig. 11. Espectro de la señal del control del Auto

En la comparación de ambos espectros se puede observar que, aunque ambas modulaciones sean OOK, presentan características diferentes. El espectro generado por la llave del auto consiste en pequeñas ráfagas fijas en la misma frecuencia, mientras que el espectro del portón es más extenso en el tiempo y presenta una variación en su frecuencia central. Esto último nos llama la atención ya que las variaciones en la frecuencia central no era el comportamiento esperado, lo asociamos a pequeñas fallas del control que afortunadamente no presentan un problema para el sistema.

Por otro lado, que la señal sea más duradera en el tiempo para el caso del control remoto del portón nos puede dar a entender que se manda varias veces la señal.

Luego de averiguar la frecuencia de ambas señales, utilizamos la herramienta Universal Radio Hacker, que nos permite capturar las señales al conectarnos al SDR HackRF.

Al grabar la señal del portón en URH, podemos observar el espectro y su codificación en bits, Figuras 13, 14. Se puede ver que efectivamente, como habíamos mencionado antes, se envían reiteradas veces el mismo código con una duración de $78.21ms$ y luego una pausa de $20.63ms$.

Al analizar más a detalle la codificación de bits obtenida del portón, se pueden observar que todas las tiras obtenidas tienen largo 85. La herramienta de análisis de protocolo de URH, nos muestra que las tramas están compuestas por una sección de sincronización (bit 1 al 32), una sección de información (bit 33 al 77) y luego un checksum (bit 78 al 85).

Al comparar con la señal de la llave del auto (que usa Rolling Code), se observan grandes diferencias. En primer lugar, el espectro en el dominio temporal es distinto, con presencias de señal más marcadas, pudiéndose distinguir seis secciones claramente definidas de distintos largos en la Figura 15.

Al analizar la codificación en bits, la señal se compone de seis secuencias de diferente longitud. La primera secuencia tiene una longitud de 8192 bits, las secuencias de la segunda a la cuarta oscilan en torno a los 2630 bits, mientras que la quinta y la sexta tienen aproximadamente 1700 bits.

Fig. 12. Espectro del control del portón

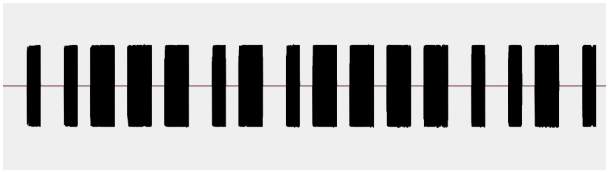

Fig. 13. Zoom-in del espectro del control del portón

Observamos que el programa URH puede identificar algunos bits de sincronización y de verificación (checksum), pero hay una larga secuencia de bits intermedios para la cual no logra determinar los campos específicos que la componen. Esto es esperable, ya que los Rolling Codes están encriptados, por lo que es coherente que un programa externo no pueda interpretar su contenido. Esta limitación está relacionada con la falta de información sobre la generación y encriptación de este tipo de códigos, ya que las empresas que desarrollan estos mecanismos suelen no divulgar detalles técnicos por razones de seguridad y confidencialidad, lo cual es justamente el objetivo de este tipo de comunicaciones.

B. Reply Attack

Luego de obtener la señal generada por el control remoto (Figura 13), se procedió a transmitirla con el objetivo de abrir y cerrar el portón sin necesidad de utilizar el dispositivo original. Para ello, URH cuenta con la herramienta ”Generate Code”, que permite emitir una señal a través del dispositivo HackerRF. Con la señal del control previamente capturada se logró hacer el Reply Attack con éxito. Se puede acceder al video del experimento que se encuentra en Drive, mediante el siguiente enlace: https://drive.google.com/file/d/1NXmcNwn-skKCVBBB2_04HxGbb_n4MGzI/view?usp=sharing

Fig. 14. Codificación en bits del portón

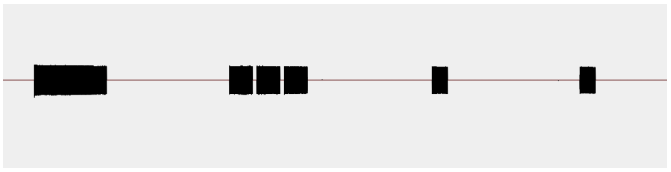

Fig. 15. Espectro de la llave del auto

IX. Referencias

[1] del Arroyo, S. N. B., Alarcón, O. C., Rivera-Suaña, J. A., & Aguilar-Montaño, L. T. (2021). Estudio de Vulnerabilidad en Transmisión ASK usando Radio Definida por Software. Revista Científica Investigación Andina, 21(1).

[2] Ghanem, A. (2022). Security Analysis of Rolling Code-based Remote Keyless Entry Systems (Doctoral dissertation).

[3] CY Wireless Technology Limited. Recuperado de https://www.rficy.com/NewsDetail.aspx?ID=161

[4] ”Garage door opener”. *Wikipedia*. Recuperado de https://en.wikipedia.org/wiki/Garage_door_opener *(*accedido el 24 de junio de 2025).

[5] 433MHz ASK signal analysis – Wireless door bell adventure, RootBSD blog. [Online]. Available: https://bytebucket.org/rootbsd/433mhz-ask-signal-analysis/raw/5f4937e4efb2198abcc375b8aefee41421941fca/pdf/433MHz_ASK_sginal_analysis-Wireless_door_bell_adventure-1.0.pdf.

[6] Great Scott Gadgets, “HackRF One,” [Online]. Available: https://greatscottgadgets.com/hackrf/one/. [Accessed: 26-Jun-2025].

[7] J. Pohl and A. Noack, “Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols,” in *Proc. 12th USENIX Workshop on Offensive Technologies (WOOT 18)*, Baltimore, MD, 2018. [Online]. Available: https://www.usenix.org/conference/woot18/presentation/pohl.

[8] “Rolling Code Overview,” ResearchGate, [Online]. Available: https://www.researchgate.net/figure/Rolling-Code-Overview_fig3_336068161.