

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE ELECTRÓNICA
VALPARAISO - CHILE



UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

**ANÁLISIS DEL CONSUMO DE POTENCIA PARA LA INGENIERÍA
INVERSA DE LA MODULACIÓN DIGITAL: UN ENFOQUE
NOVEDOSO PARA ATAQUES EN LA CAPA FÍSICA DE SISTEMAS DE
COMUNICACIÓN**

PABLO TRONCOSO PAREJA

**MEMORIA DE TITULACIÓN PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL TELEMÁTICO**

PROFESOR GUÍA : GONZALO CARVAJAL
PROFESOR CORREFERENTE : JOSÉ MANUEL MARTÍNEZ

JUNIO 2026



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Análisis del consumo de potencia para la ingeniería inversa de la modulación digital: un enfoque novedoso

Título del trabajo: para ataques en la capa física de sistemas de comunicación

Nombre del candidato(a): Pablo Troncoso Pareja

Carrera / Grado: Ingeniería Civil Telemática

Campus: Casa Central

Departamento: Electrónica

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Gonzalo Carvajal Barrera, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 7 de octubre de 2026

Firma: 

Estudiante o Candidato(a):

Fecha: 7 de octubre de 2026

Firma: 

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

Agradecimientos

Este trabajo es la culminación de muchos años de estudio, no solo en la Universidad Federico Santa María, sino también en la escuela de ingeniería IMT Atlantique (Francia), donde pude realizar mi doble título en Ingeniería en Sistemas Embebidos, durante el cual se desarrolló este trabajo.

Este doble título no hubiera sido posible sin el apoyo de mi familia, que me acompañó en cada paso y en cada dificultad. Esta experiencia, llena de desafíos, logró abrirme las puertas a un nuevo mundo de conocimiento y trabajo del que hoy formo parte; por ello, también agradezco profundamente a la Universidad por haberme dado la oportunidad de realizar este doble título.

Mención especial

Este trabajo de memoria se desarrolló a partir del trabajo de investigación realizado en la escuela de ingeniería IMT Atlantique, en Brest, Francia, bajo la tutoría del Dr. Yehya Nasser.

Los resultados se encuentran publicados en el artículo: *P. Pareja, Y. Nasser, A. Masmoudi, and S. Houcke, “Power consumption analysis for reverse engineering digital modulation: A novel approach to physical layer attacks on communication systems,” in Cybersecurity (I. Praça, S. Bernardi, and P. R. Inácio, eds.), (Cham), pp. 52–62, Springer Nature Switzerland, 2025. [1]*, presentado en la novena conferencia interdisciplinaria europea de ciberseguridad (9th European Interdisciplinary Cybersecurity Conference, EICC 2025, Rennes, France, June 18–19, 2025, Proceedings).

Lo presentado en este escrito corresponde a extractos del artículo mencionado.

Índice general

1. Introducción	5
1.1. Motivación y contexto	5
1.2. Planteamiento del problema y objetivos	6
1.3. Estructura del documento	7
2. Antecedentes	8
2.1. Modulación digital	8
2.2. Consumo de potencia en circuitos digitales	11
2.3. Análisis por canal lateral	12
2.4. Extracción de características	13
2.5. Clasificación mediante aprendizaje automático	13
2.6. Síntesis	14
2.7. Estado del arte	14
2.7.1. Clasificación de modulación	14
2.7.2. Ataques por canal lateral de potencia	15
3. Metodología	17
3.1. Configuración del sistema de medición	17
3.2. Arquitectura del sistema y modelo propuesto	19
3.3. Caracterización y adquisición de potencia	20
3.4. Procesamiento y análisis de datos	21
4. Resultados	23
4.1. Análisis estadístico	23
4.2. Clasificación de esquemas de modulación	25
4.3. Discusión de los resultados	26
5. Conclusiones	29

Índice de figuras

2.1. Elementos básicos de la comunicación digital	9
2.2. Ejemplo de señal modulada mediante ASK (OOK) en el dominio del tiempo. . .	9
2.3. Ejemplo de señal modulada mediante FSK, donde la frecuencia cambia según el símbolo transmitido.	10
2.4. Ejemplo de señal modulada mediante 16-QAM	10
2.5. Constelación de una modulación 16-QAM en el plano I/Q.	11
3.1. CW305	18
3.2. Modelo para la adquisición de datos.	20
4.1. Media, desviación estándar, asimetría y curtosis para los distintos métodos de modulación con muestreo sincrónico a una muestra por ciclo de reloj.	24
4.2. Desviación estándar para los distintos métodos de modulación con muestreo asincrónico a dos muestras por ciclo de reloj.	25
4.3. Matrices de confusión para la clasificación de modulaciones mediante XGBoost en los distintos escenarios de adquisición.	28

1 | Introducción

Los sistemas modernos de comunicaciones digitales se encuentran presentes en prácticamente todos los ámbitos tecnológicos, desde redes móviles y dispositivos IoT hasta aplicaciones aeroespaciales y sistemas de defensa. El correcto funcionamiento de estos sistemas depende de múltiples etapas de procesamiento digital que permiten transmitir información de forma eficiente y fiable a través de distintos medios físicos.

Dentro de este contexto, la identificación de las características de una transmisión constituye un problema de gran interés tanto para fines de monitorización como de seguridad. La capacidad de determinar cómo opera un sistema de comunicación permite comprender su funcionamiento interno, detectar posibles interferencias y, en determinados escenarios, evaluar su nivel de vulnerabilidad frente a técnicas de ingeniería inversa.

Tradicionalmente, el análisis de sistemas de comunicación se ha centrado en el estudio de las señales de radiofrecuencia transmitidas. Sin embargo, los avances recientes en el ámbito de la seguridad de hardware han demostrado que la implementación física de un sistema también puede revelar información relevante sobre las operaciones que realiza. Esta observación abre la posibilidad de estudiar sistemas de comunicación desde una perspectiva diferente, centrada no en la señal transmitida, sino en las características físicas del dispositivo que la genera.

1.1. Motivación y contexto

La identificación de señales provenientes de fuentes desconocidas o parcialmente conocidas constituye un problema fundamental en telecomunicaciones, especialmente en aplicaciones relacionadas con seguridad, inteligencia, vigilancia del espectro radioeléctrico y guerra electrónica [2]. En estos escenarios, una señal interceptada puede contener información valiosa acerca de su frecuencia portadora, ancho de banda, esquema de codificación, número de portadoras y, particularmente, el tipo de modulación utilizado.

La clasificación de modulación consiste en determinar automáticamente el esquema de modulación empleado por una señal sin disponer de información previa sobre el transmisor. Esta tarea es considerada un paso fundamental para comprender el funcionamiento de un sistema de comunicación, ya que el conocimiento de la modulación permite posteriormente abordar procesos más complejos como la demodulación, la decodificación o la identificación de protocolos de comunicación.

La relevancia de este problema es especialmente evidente en aplicaciones militares y de seguridad. La incapacidad de identificar correctamente la modulación utilizada puede impedir

la recuperación de la información transmitida, mientras que conocer dicho esquema puede facilitar tareas de vigilancia, análisis o incluso la generación de interferencias deliberadas sobre el sistema objetivo.

Los métodos convencionales de clasificación de modulación se basan en el análisis de la señal de radiofrecuencia interceptada [3, 4]. Si bien estas técnicas han alcanzado niveles elevados de precisión en condiciones favorables, su rendimiento suele degradarse significativamente cuando la relación señal a ruido es baja o cuando la señal observada presenta distorsiones importantes. Esta limitación motiva la búsqueda de fuentes alternativas de información que permitan complementar o incluso reemplazar el análisis tradicional de radiofrecuencia en determinados escenarios.

Paralelamente, el campo de la seguridad de hardware ha demostrado que los sistemas digitales generan fugas de información involuntarias durante su funcionamiento. Estas fugas, conocidas como canales laterales (*side-channels*), pueden manifestarse a través del consumo de potencia, emisiones electromagnéticas, tiempos de ejecución u otras características físicas observables. El análisis de estas señales ha sido ampliamente utilizado en criptografía para recuperar información sensible, demostrando que el comportamiento físico de un circuito puede revelar detalles relevantes sobre las operaciones que realiza.

Entre las distintas fuentes de fuga existentes, el consumo de potencia resulta particularmente interesante debido a su estrecha relación con la actividad interna de los circuitos digitales. El estudio de este tipo de fugas corresponde a la seguridad en la capa física del sistema y constituye la principal preocupación de este trabajo. Estudios previos han demostrado que el consumo dinámico depende de factores como la frecuencia de operación, la arquitectura utilizada y, especialmente, los datos procesados por el sistema [5]. Asimismo, se ha observado que diferentes esquemas de modulación pueden generar perfiles de consumo distintos [6]. Estas observaciones sugieren que el consumo de potencia podría contener información suficiente para identificar el tipo de modulación implementado, incluso sin necesidad de observar la señal de radiofrecuencia transmitida.

1.2. Planteamiento del problema y objetivos

A partir del contexto descrito anteriormente, surge la siguiente pregunta de investigación:

¿Es posible identificar el esquema de modulación digital utilizado por un sistema únicamente a partir de su consumo de potencia?

Responder esta pregunta permitiría determinar si el consumo de potencia constituye una fuente de información explotable para la clasificación de modulación y, en consecuencia, si representa una potencial vulnerabilidad desde la perspectiva de la seguridad física de los sistemas de comunicación.

El objetivo general de este trabajo es demostrar que diferentes esquemas de modulación digital generan patrones de consumo de potencia distinguibles y que dichas diferencias pueden utilizarse para desarrollar un sistema automático de clasificación.

Para alcanzar este objetivo, se implementan distintos moduladores digitales sobre una plataforma FPGA (*Field-Programmable Gate Array*) y se adquieren trazas de consumo de potencia

durante su operación. Posteriormente, estas trazas son analizadas mediante técnicas estadísticas y utilizadas para entrenar modelos de aprendizaje automático capaces de identificar la modulación correspondiente.

De manera específica, este trabajo contempla los siguientes objetivos:

- Implementar distintos esquemas de modulación digital sobre una plataforma FPGA.
- Diseñar un entorno experimental para la adquisición de trazas de consumo de potencia.
- Analizar estadísticamente las características de las trazas obtenidas.
- Extraer características representativas a partir de los datos de consumo.
- Desarrollar un modelo de clasificación basado en aprendizaje automático.
- Evaluar el rendimiento del sistema bajo distintas condiciones de adquisición.

El alcance de esta investigación se limita al estudio de moduladores digitales implementados en FPGA y al análisis del consumo de potencia del lado transmisor. Asimismo, las mediciones se realizan en un entorno controlado utilizando acceso directo a las líneas de alimentación del dispositivo. Por lo tanto, el objetivo principal no es desarrollar un ataque práctico contra sistemas comerciales, sino demostrar la existencia y explotabilidad de la información presente en este canal lateral.

1.3. Estructura del documento

El resto de esta memoria se organiza de la siguiente manera.

El Capítulo 2 presenta los antecedentes y el marco teórico necesario para comprender los conceptos fundamentales utilizados en el desarrollo del trabajo, incluyendo modulación digital, consumo de potencia en circuitos digitales, análisis por canal lateral y técnicas básicas de aprendizaje automático. Asimismo, se revisa el estado del arte relacionado con la clasificación automática de modulación y con los ataques por canal lateral basados en consumo de potencia, identificando las principales contribuciones y limitaciones existentes en la literatura.

El Capítulo 3 describe la metodología desarrollada, incluyendo la plataforma experimental utilizada, la implementación de los moduladores digitales, el sistema de adquisición de trazas de potencia y los procedimientos de procesamiento y clasificación de datos.

El Capítulo 4 presenta los resultados experimentales obtenidos y analiza el desempeño de los modelos de clasificación bajo las distintas condiciones evaluadas.

Finalmente, el Capítulo 5 expone las conclusiones del trabajo, resume las principales contribuciones realizadas y propone posibles líneas de investigación futuras.

2 | Antecedentes

Este capítulo presenta los fundamentos teóricos necesarios para comprender el trabajo desarrollado. Se abordan los conceptos clave relacionados con la modulación digital, el consumo de potencia en circuitos digitales, el análisis por canal lateral y las técnicas de extracción de características utilizadas en el estudio. Finalmente, se presenta el estado del arte de las dos principales áreas investigadas.

2.1. Modulación digital

La transmisión de información a través de medios físicos constituye uno de los pilares fundamentales de los sistemas modernos de telecomunicaciones. Ya sea en redes móviles, sistemas satelitales, dispositivos IoT o enlaces inalámbricos de corto alcance, la información digital debe transformarse en señales capaces de propagarse eficientemente a través de un canal de comunicación.

Esta transformación se realiza mediante un proceso denominado modulación. En términos generales, la modulación consiste en utilizar una señal portadora, normalmente una onda sinusoidal de frecuencia elevada, para transportar la información deseada. Los datos digitales modifican determinadas características de dicha portadora, permitiendo que la información pueda ser transmitida y posteriormente recuperada por un receptor.

La elección del esquema de modulación tiene un impacto directo sobre el rendimiento del sistema de comunicación. Diferentes técnicas ofrecen distintos compromisos entre eficiencia espectral, robustez frente al ruido, complejidad de implementación y consumo energético. Debido a ello, la modulación constituye una de las etapas más relevantes dentro de cualquier sistema de comunicaciones digitales.

En la Figura 2.1 se muestra dónde se sitúa la modulación dentro del proceso de comunicación digital.

Dependiendo del parámetro de la portadora que se modifique, se distinguen distintos tipos de modulación. A continuación, se detallan los esquemas analizados en este trabajo.

La modulación por desplazamiento de amplitud (*Amplitude Shift Keying*, ASK) [7] es una de las formas más simples de modulación digital. En este esquema, la información se transmite modificando la amplitud de una señal portadora. Cuando se utilizan únicamente dos niveles de amplitud, el receptor puede asociar cada nivel a un valor lógico diferente.

Un caso particular ampliamente utilizado es la modulación OOK (*On-Off Keying*), donde la

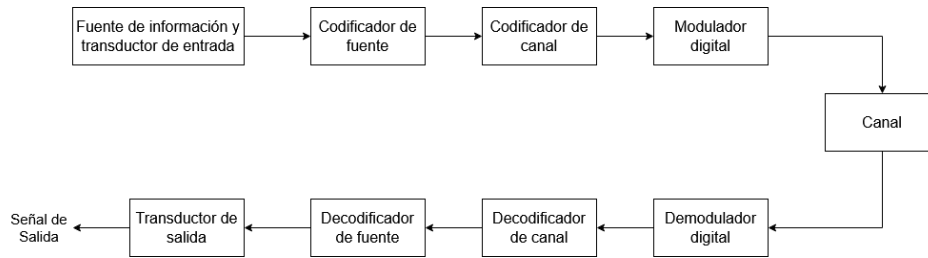


Figura 2.1: Elementos básicos de la comunicación digital

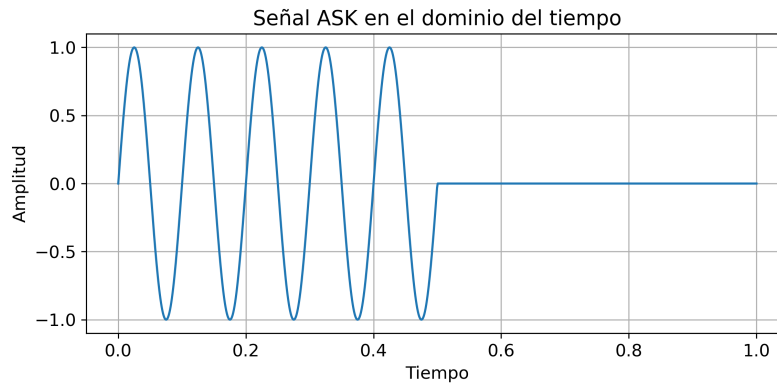


Figura 2.2: Ejemplo de señal modulada mediante ASK (OOK) en el dominio del tiempo.

presencia de la portadora representa un símbolo y su ausencia representa el otro. Un ejemplo de una señal modulada entre estos dos símbolos se muestra en la Figura 2.2. Debido a su simplicidad, este esquema se emplea en sistemas de bajo costo y bajo consumo energético. Sin embargo, al depender directamente de la amplitud de la señal, resulta especialmente vulnerable a perturbaciones e interferencias presentes en el canal de comunicación.

En la modulación por desplazamiento de frecuencia (*Frequency Shift Keying*, FSK), la información se representa mediante cambios discretos en la frecuencia de la señal portadora. Cada símbolo se asocia a una frecuencia distinta. Por ejemplo, en la Figura 2.3 se muestra el caso de 2-FSK, donde se representan dos símbolos que se diferencian por la frecuencia de la portadora. Este esquema es más robusto frente al ruido que ASK, pero requiere un mayor ancho de banda.

La modulación de amplitud en cuadratura (*Quadrature Amplitude Modulation*, QAM) combina variaciones en la amplitud y la fase de la señal. La señal transmitida puede representarse mediante dos componentes: en fase (I) y en cuadratura (Q).

En la Figura 2.4 se observa cómo puede representarse la señal en el tiempo, donde tanto su amplitud como su fase cambian, y cada combinación representa un símbolo distinto. A mayor orden de modulación (como en el caso de 64-QAM y 256-QAM), mayores son las combinaciones posibles y más información puede transmitirse por símbolo, a cambio de una mayor susceptibilidad a errores.

El orden de modulación se refiere al número de símbolos distintos que pueden transmitirse. A mayor orden, mayor cantidad de información por símbolo, pero también mayor susceptibilidad a errores. Este compromiso entre eficiencia y robustez es fundamental en sistemas de

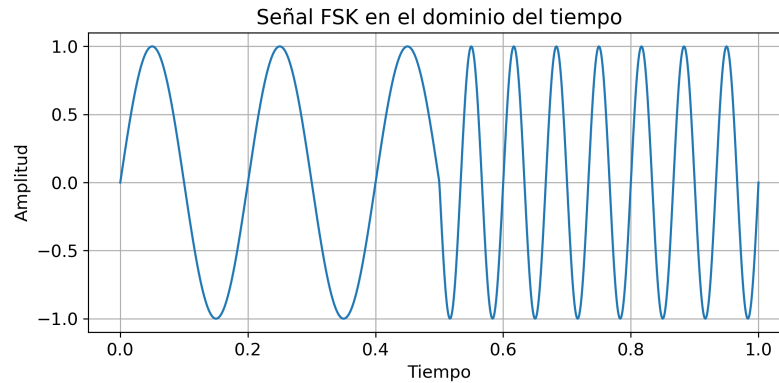


Figura 2.3: Ejemplo de señal modulada mediante FSK, donde la frecuencia cambia según el símbolo transmitido.

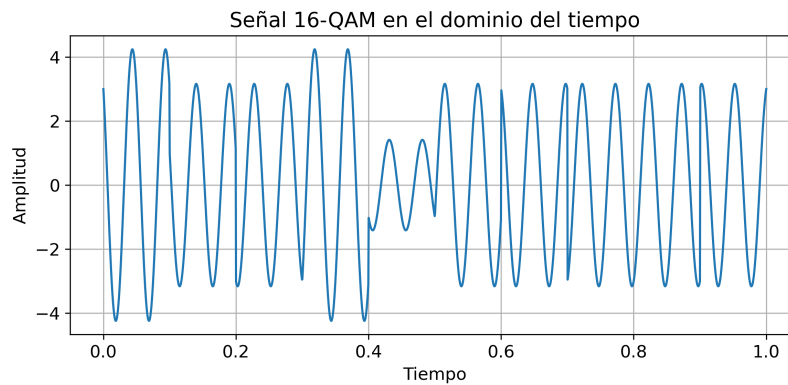


Figura 2.4: Ejemplo de señal modulada mediante 16-QAM

comunicación.

Los esquemas QAM de orden elevado (por ejemplo, 64-QAM o 256-QAM) permiten transmitir más bits por símbolo, aumentando la eficiencia espectral. Sin embargo, son más sensibles al ruido debido a la proximidad entre los puntos de la constelación.

La constelación para el caso de 16-QAM se ve representada en la Figura 2.5, donde cada punto es un símbolo diferente que puede representarse como una combinación de su componente en fase (I) y su componente en cuadratura (Q).

La principal ventaja de QAM radica en su elevada eficiencia espectral. Mientras que esquemas simples como ASK o FSK transmiten una cantidad limitada de información por símbolo, QAM permite representar múltiples bits utilizando simultáneamente variaciones de amplitud y fase.

Sin embargo, este aumento en la capacidad de transmisión implica un mayor desafío para el receptor. A medida que aumenta el orden de modulación, los puntos de la constelación se encuentran más próximos entre sí, reduciendo la tolerancia frente al ruido y las distorsiones introducidas por el canal.

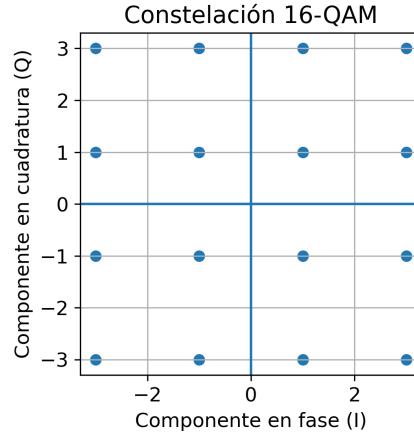


Figura 2.5: Constelación de una modulación 16-QAM en el plano I/Q.

2.2. Consumo de potencia en circuitos digitales

Cuando una señal digital cambia de un estado lógico bajo a uno alto, o viceversa, los transistores involucrados deben cargar y descargar capacitancias internas. Este proceso requiere energía y genera variaciones instantáneas en el consumo de potencia. Como consecuencia, dos operaciones distintas ejecutadas sobre los mismos recursos hardware pueden producir perfiles energéticos diferentes. De manera similar, una misma operación aplicada sobre conjuntos de datos distintos también puede generar patrones de consumo diferentes.

Este fenómeno constituye la base física de los ataques por canal lateral de potencia. Si las variaciones observadas son suficientemente consistentes, es posible inferir información sobre las operaciones realizadas por el sistema únicamente observando su consumo energético.

El consumo de potencia en circuitos digitales, como las FPGA, se divide principalmente en dos componentes: potencia estática y potencia dinámica.

La potencia estática corresponde al consumo presente incluso cuando el circuito no está realizando operaciones. Está asociada principalmente a corrientes de fuga en los transistores.

La potencia dinámica es la componente dominante en circuitos digitales activos y está directamente relacionada con el factor de actividad de los transistores. Puede expresarse de forma simplificada como:

$$P_{din} \propto C \cdot V^2 \cdot f \cdot \alpha$$

donde:

- (C) es la capacitancia de carga,
- (V) es la tensión de alimentación,
- (f) es la frecuencia de operación,
- (α) es el factor de actividad.

Este modelo muestra que el consumo de potencia depende directamente de los datos procesados, ya que estos determinan el factor de actividad (α). Por lo tanto, diferentes operaciones (como distintos esquemas de modulación) pueden generar patrones de consumo diferenciables.

2.3. Análisis por canal lateral

Los sistemas digitales no solo producen los resultados para los cuales fueron diseñados, sino que también generan diversas manifestaciones físicas durante su funcionamiento. Estas manifestaciones, conocidas como canales laterales (*side-channels*), corresponden a fugas de información no intencionadas que pueden revelar detalles sobre las operaciones internas realizadas por el dispositivo. El estudio y explotación de estas fugas constituye el área conocida como Análisis por Canal Lateral (*Side-Channel Analysis*, SCA).

A diferencia de los métodos tradicionales de análisis, que buscan acceder directamente a los datos o algoritmos implementados, los ataques por canal lateral se basan en la observación de fenómenos físicos asociados a la ejecución del sistema. Entre las fuentes de información más utilizadas se encuentran el consumo de potencia, las emisiones electromagnéticas, los tiempos de ejecución y, en algunos casos, incluso señales acústicas producidas por el hardware. Aunque estas fugas son consecuencia natural del funcionamiento de los circuitos electrónicos, pueden contener información suficiente para inferir aspectos relevantes sobre los datos procesados o las operaciones realizadas.

El análisis por canal lateral ha sido ampliamente estudiado en el ámbito de la criptografía, donde se ha demostrado que es posible recuperar claves secretas observando únicamente el comportamiento físico de un dispositivo durante la ejecución de algoritmos como AES o RSA. Estos resultados han puesto de manifiesto que la seguridad de un sistema no depende exclusivamente de la solidez matemática de los algoritmos utilizados, sino también de las características físicas de su implementación.

Dentro de las distintas técnicas de SCA, el análisis basado en consumo de potencia ocupa un lugar especialmente relevante. Como se discutió en la sección anterior, el consumo de potencia dinámica de un circuito digital depende directamente de la actividad de sus transistores. Cada vez que una señal lógica cambia de estado, se produce una transferencia de carga que genera un consumo energético medible. En consecuencia, existe una relación entre los datos procesados, las operaciones ejecutadas y la potencia consumida por el dispositivo.

Esta dependencia entre actividad lógica y consumo energético constituye el fundamento físico de los ataques por análisis de potencia. Si diferentes algoritmos o conjuntos de datos generan patrones de actividad distintos, es posible que dichas diferencias se reflejen en las trazas de consumo observadas. En el contexto de este trabajo, esta misma idea se aplica para estudiar si distintos esquemas de modulación digital producen patrones de consumo suficientemente característicos como para permitir su identificación.

Otro aspecto importante en el análisis de potencia es la forma en que se adquieren las mediciones. Una estrategia consiste en realizar muestreo sincrónico, donde las muestras de potencia se capturan sincronizadas con el reloj interno del sistema. Esta aproximación permite observar con mayor precisión la actividad asociada a cada ciclo de operación, reduciendo la incertidumbre temporal y facilitando el análisis posterior de las trazas.

Por el contrario, en el muestreo asincrónico no existe una relación fija entre la frecuencia de muestreo y el reloj del dispositivo analizado. Como resultado, las operaciones internas pueden aparecer desplazadas temporalmente entre distintas adquisiciones, introduciendo ruido adicional y dificultando la identificación de patrones repetitivos. Sin embargo, este escenario suele ser más representativo de situaciones reales, donde el reloj interno del sistema objetivo no siempre está disponible para el atacante.

La comparación entre ambos enfoques constituye uno de los aspectos centrales de esta investigación, ya que permite evaluar hasta qué punto la sincronización influye en la capacidad de identificar esquemas de modulación a partir de información obtenida mediante análisis de potencia.

2.4. Extracción de características

Una traza de potencia individual puede contener miles de muestras. Utilizar directamente todas estas muestras como entrada de un clasificador puede aumentar la complejidad computacional y dificultar la identificación de patrones relevantes. Por esta razón, es habitual resumir la información contenida en la señal mediante un conjunto reducido de características representativas.

En este trabajo se utilizan los primeros cuatro momentos estadísticos:

- Media
- Desviación estándar
- Asimetría
- Curtosis

Estos parámetros permiten describir la distribución de los valores de la señal, capturando información relevante sobre su forma y variabilidad.

La extracción de características permite:

- Reducir la complejidad computacional
- Eliminar ruido
- Resaltar patrones relevantes

Si bien existen métodos más avanzados, como el Análisis de Componentes Principales (PCA), los momentos estadísticos ofrecen una solución simple y eficaz para un análisis inicial.

2.5. Clasificación mediante aprendizaje automático

El problema abordado en este trabajo puede formularse como una tarea de clasificación supervisada, donde el objetivo es asignar a cada traza de potencia una etiqueta correspondiente al esquema de modulación.

Los modelos basados en árboles de decisión dividen el espacio de características en regiones mediante reglas simples. El método de *boosting* consiste en combinar múltiples árboles débiles para construir un modelo más robusto.

XGBoost es un algoritmo de *gradient boosting* ampliamente utilizado por su eficiencia y rendimiento. Es capaz de capturar relaciones no lineales entre las características, lo que lo hace especialmente adecuado para este tipo de problema.

Para evaluar el rendimiento del modelo se utilizan las siguientes métricas:

- Exactitud
- Precisión
- Exhaustividad
- Puntuación F1

Estas métricas permiten evaluar el modelo desde diferentes perspectivas, proporcionando una visión completa de su desempeño.

2.6. Síntesis

En conjunto, los conceptos presentados en este capítulo permiten comprender cómo el consumo de potencia en un sistema digital puede contener información relevante sobre las operaciones que realiza. La combinación de técnicas de análisis de canal lateral, extracción de características y aprendizaje automático constituye la base del enfoque propuesto en este trabajo.

2.7. Estado del arte

A continuación se detalla el estado del arte de los dos principales temas tratados anteriormente, destacando los últimos avances en cada área.

2.7.1. Clasificación de modulación

La Clasificación Automática de Modulación (AMC, del inglés *Automatic Modulation Classification*) constituye un elemento fundamental en los sistemas modernos de comunicación digital. Su objetivo es identificar automáticamente el esquema de modulación empleado por una señal recibida sin conocimiento previo del transmisor. Esta capacidad es esencial en múltiples aplicaciones, que abarcan desde sistemas militares e inteligencia hasta aplicaciones civiles como la gestión del espectro y la monitorización de redes inalámbricas [8].

Los métodos de AMC pueden clasificarse principalmente en dos grandes categorías: los enfoques basados en verosimilitud (*likelihood-based*) y los enfoques basados en características (*feature-based*) [4].

Los métodos basados en verosimilitud se fundamentan en modelos probabilísticos de la señal recibida. En estos enfoques, se calcula la probabilidad de que una señal observada haya sido generada por un determinado esquema de modulación, y se selecciona aquel que maximiza dicha

probabilidad. Aunque estos métodos pueden ofrecer un rendimiento óptimo en condiciones ideales, presentan una elevada complejidad computacional y requieren un conocimiento preciso del canal de transmisión y del ruido, lo que limita su aplicabilidad en escenarios reales.

Por otro lado, los métodos basados en características consisten en extraer parámetros representativos de la señal (por ejemplo, estadísticas de orden superior, propiedades espectrales o características en el dominio del tiempo) y utilizar estos parámetros como entrada para un clasificador. Estos enfoques son generalmente más robustos frente a incertidumbres del canal y presentan menor complejidad computacional, lo que los hace más adecuados para implementaciones prácticas.

En los últimos años, el uso de técnicas de aprendizaje automático y aprendizaje profundo ha permitido mejorar significativamente el rendimiento de los sistemas de AMC. Modelos como redes neuronales convolucionales (CNN) o recurrentes (RNN) han demostrado una gran capacidad para aprender representaciones complejas directamente a partir de los datos. Sin embargo, estos métodos suelen requerir grandes volúmenes de datos de entrenamiento y una elevada capacidad de cómputo.

A pesar de estos avances, uno de los principales desafíos de la AMC sigue siendo su sensibilidad a la relación señal a ruido (SNR). En condiciones de baja SNR, el rendimiento de los clasificadores se degrada significativamente [3], [9]. En particular, muchos modelos presentan precisiones inferiores al 60 % cuando la SNR es menor o igual a 0 dB, mientras que pueden superar el 90 % en condiciones más favorables. Esta dependencia limita su uso en entornos reales, donde las señales suelen estar afectadas por ruido, interferencias o desvanecimientos del canal.

Otro factor que incrementa la dificultad del problema es el uso de esquemas de modulación de orden elevado, como QAM de alta densidad. En estos casos, las constelaciones presentan puntos muy próximos entre sí, lo que hace que pequeñas perturbaciones debidas al ruido puedan provocar errores significativos en la clasificación.

Adicionalmente, las técnicas modernas de seguridad en la capa física introducen nuevos retos para la AMC. Métodos como la modulación direccional (*Directional Modulation*, DM), la modulación espacial (*Spatial Modulation*, SM), las comunicaciones encubiertas (*covert communications*) o el uso de superficies reflectantes inteligentes (*Intelligent Reflecting Surface*, IRS) [10] permiten ocultar o distorsionar la señal de manera que dificultan su interceptación y análisis. Estas técnicas reducen aún más la eficacia de los métodos tradicionales de clasificación de modulación.

En conjunto, estas limitaciones ponen de manifiesto la necesidad de explorar enfoques alternativos que no dependan exclusivamente de la observación directa de la señal de radiofrecuencia.

2.7.2. Ataques por canal lateral de potencia

Como alternativa a los enfoques tradicionales basados en la señal transmitida, los ataques por canal lateral (*Side-Channel Attacks*, SCA) explotan información filtrada por la implementación física de los sistemas electrónicos [11]. Estas fugas de información no intencionadas pueden proporcionar indicios sobre los procesos internos de un sistema, incluso cuando los datos procesados o transmitidos no son directamente accesibles.

Entre los principales tipos de canales laterales se encuentran el consumo de potencia, las emisiones electromagnéticas, los tiempos de ejecución y, en algunos casos, incluso las emisiones acústicas. De todos ellos, el análisis del consumo de potencia ha sido uno de los más estudiados debido a su relativa facilidad de medición y a la gran cantidad de información que puede revelar.

Los ataques basados en consumo de potencia han sido ampliamente investigados en el ámbito de la criptografía, donde se utilizan para extraer claves secretas de dispositivos seguros. Entre las técnicas más conocidas se encuentran el análisis de potencia simple (*Simple Power Analysis*, SPA), el análisis de potencia diferencial (*Differential Power Analysis*, DPA), los ataques por plantilla (*template attacks*) y el análisis de potencia por correlación (*Correlation Power Analysis*, CPA) [12]. Estas técnicas se basan en la observación de patrones en las trazas de consumo que están correlacionados con los datos procesados por el dispositivo.

En esencia, muchos de estos ataques pueden formularse como problemas de clasificación o de estimación estadística. En este contexto, las técnicas de aprendizaje automático han emergido como herramientas especialmente adecuadas para el análisis de canales laterales [13], [14]. Mediante la extracción de características relevantes a partir de las trazas de consumo, es posible entrenar modelos capaces de identificar patrones complejos y de inferir información sobre los procesos internos del sistema.

A pesar de su amplio uso en criptografía, la aplicación de técnicas de análisis de canal lateral al problema de la clasificación de modulación ha sido poco explorada. En particular, el uso del consumo de potencia como fuente de información para inferir el esquema de modulación representa una línea de investigación emergente. Este enfoque presenta varias ventajas potenciales, entre las que destaca su independencia respecto a la calidad de la señal de radiofrecuencia, lo que podría permitir su uso en escenarios donde los métodos tradicionales de AMC fallan.

En este contexto, el presente trabajo se sitúa en la intersección entre la clasificación de modulación y el análisis de canales laterales, proponiendo un enfoque novedoso basado en el análisis de consumo de potencia para la identificación de esquemas de modulación digital.

3 | Metodología

El presente capítulo describe la metodología empleada para evaluar la posibilidad de identificar esquemas de modulación digital a partir de información obtenida mediante análisis de potencia. Para ello, se detalla la plataforma experimental utilizada, la arquitectura implementada sobre FPGA, el proceso de adquisición de datos y las técnicas de procesamiento y clasificación aplicadas posteriormente.

El objetivo principal de esta metodología es garantizar que las diferencias observadas en las trazas de consumo de potencia puedan atribuirse al esquema de modulación utilizado y no a otros factores externos. Asimismo, se busca construir un conjunto de datos suficientemente diverso para evaluar la robustez del enfoque propuesto bajo distintas condiciones de operación.

3.1. Configuración del sistema de medición

Uno de los principales desafíos de este trabajo consiste en adquirir mediciones de consumo de potencia con una resolución suficiente para detectar diferencias sutiles entre distintos esquemas de modulación digital. A diferencia de los métodos tradicionales de clasificación de modulación, donde la información se obtiene directamente a partir de la señal de radiofrecuencia transmitida, en este estudio la información de interés se encuentra en la actividad interna del hardware encargado de generar dicha señal. Como consecuencia, resulta necesario utilizar una plataforma capaz de capturar trazas de potencia de forma precisa y repetible.

Para este propósito se empleó la plataforma ChipWhisperer (CW) [15], ampliamente utilizada en investigación de seguridad hardware y análisis por canal lateral. Una de las principales ventajas de esta plataforma es que integra en un único sistema tanto el dispositivo objetivo como la infraestructura necesaria para la adquisición de potencia, simplificando considerablemente el desarrollo experimental.

La configuración utilizada está compuesta por una tarjeta objetivo CW305 y una tarjeta de captura CW-Lite, tal como se muestra en la Figura 3.1. La tarjeta CW305 incorpora una FPGA Artix-7 sobre la cual se implementaron los distintos esquemas de modulación estudiados. Por su parte, la tarjeta CW-Lite se encarga de la adquisición de las trazas de potencia y de la sincronización del proceso de captura.

La FPGA puede configurarse mediante un microcontrolador ARM integrado en la plataforma. A través de esta interfaz es posible programar el dispositivo, ajustar parámetros de operación, configurar el PLL (*Phase-Locked Loop*) interno y transferir datos desde un computador

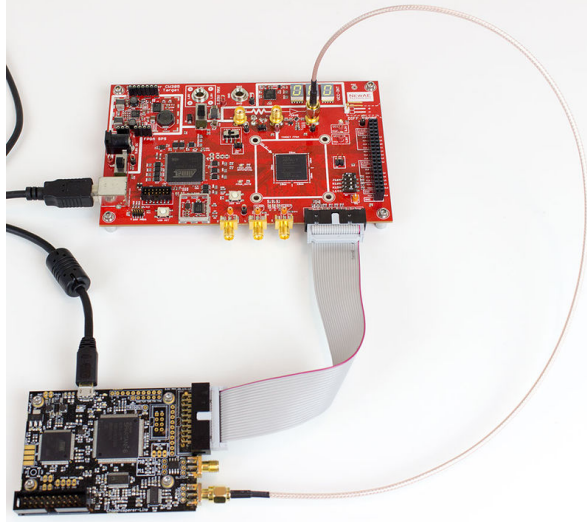


Figura 3.1: Configuración experimental utilizada para la adquisición de trazas de potencia.

externo. Esta capacidad resulta especialmente útil para automatizar experimentos que requieren modificar sistemáticamente distintos parámetros de configuración.

La interacción con la plataforma se realizó mediante Python utilizando cuadernos Jupyter. Con el fin de facilitar la ejecución de campañas experimentales extensas, se desarrolló un conjunto de scripts que permiten automatizar la programación de la FPGA, la generación de datos de entrada, la adquisición de trazas y el almacenamiento de resultados.

La tarjeta CW-Lite incorpora un convertidor analógico-digital (ADC) de 10 bits capaz de operar a frecuencias de muestreo de hasta 105 MS/s. Una característica particularmente relevante es la posibilidad de realizar muestreo sincrónico, donde la adquisición se encuentra alineada con el reloj interno de la FPGA. Este tipo de muestreo permite capturar de forma más precisa la actividad interna del circuito y ha demostrado ser especialmente beneficioso en aplicaciones de análisis de potencia [16].

Sin embargo, el muestreo sincrónico presenta ciertas limitaciones prácticas. En particular, la frecuencia de muestreo debe mantener una relación fija con la frecuencia de reloj del dispositivo objetivo, restringiendo la flexibilidad del sistema. Debido a ello, además del escenario ideal de muestreo sincrónico, también se consideró un escenario de muestreo asincrónico donde la frecuencia de adquisición puede seleccionarse independientemente del reloj de la FPGA.

La comparación entre ambos escenarios constituye un aspecto importante de esta investigación. Mientras que el muestreo sincrónico representa una situación favorable para el atacante, donde existe acceso a información temporal precisa sobre el sistema objetivo, el muestreo asincrónico representa un escenario más realista donde dicha sincronización no está disponible.

Finalmente, se decidió variar la frecuencia de operación de la FPGA durante los experimentos. Esta decisión se basa en que numerosos dispositivos embebidos modernos emplean mecanismos de escalado dinámico de frecuencia con el objetivo de optimizar el consumo energético. Evaluar distintas frecuencias permite determinar si las características extraídas permanecen discriminantes incluso bajo cambios en las condiciones de operación del dispositivo.

3.2. Arquitectura del sistema y modelo propuesto

La infraestructura experimental desarrollada se basa en un proyecto existente del ecosistema ChipWhisperer [17], originalmente diseñado para la ejecución del algoritmo criptográfico AES. Este proyecto fue seleccionado debido a que ya incorpora una arquitectura completa para la adquisición sincronizada de trazas de potencia, permitiendo reutilizar gran parte de la infraestructura experimental existente.

La lógica correspondiente al algoritmo AES fue reemplazada por un bloque de modulación digital desarrollado específicamente para este trabajo. De esta forma, se mantuvo la compatibilidad con el sistema de captura mientras se adaptaba la funcionalidad al problema de investigación planteado.

El flujo general de procesamiento implementado en la FPGA puede dividirse en cuatro etapas principales, expuestas en el diagrama de la Figura 3.2. En primer lugar, los datos generados desde la interfaz Python son transferidos hacia la FPGA mediante un transmisor serial. Posteriormente, estos datos son procesados por el bloque de modulación correspondiente. Los símbolos generados son almacenados temporalmente en memoria RAM y finalmente recuperados para su validación y análisis.

La incorporación de memoria RAM dentro de la arquitectura cumple un papel importante. Sin este mecanismo, el procesamiento quedaría limitado por la velocidad de comunicación entre el computador y la FPGA. Al almacenar temporalmente los resultados en memoria interna, todo el proceso de modulación puede ejecutarse a la máxima velocidad permitida por el reloj del dispositivo, permitiendo que las mediciones reflejen únicamente el comportamiento del hardware implementado.

Los esquemas de modulación implementados fueron seleccionados con el objetivo de cubrir distintas familias de modulación digital y distintos órdenes de complejidad. En particular, se implementaron las siguientes modulaciones:

- OOK, 4-ASK y 16-ASK.
- 4-FSK y 16-FSK.
- 4-QAM, 16-QAM, 64-QAM y 256-QAM.

La inclusión de distintos órdenes de modulación permite estudiar cómo la complejidad del esquema afecta los patrones de consumo de potencia observados.

En el caso de las modulaciones QAM se desarrollaron dos implementaciones distintas. La primera utiliza tablas de consulta (LUTs) para determinar los valores de las componentes I y Q, mientras que la segunda calcula dichos valores mediante operaciones aritméticas. Aunque ambas implementaciones generan exactamente la misma constelación de símbolos, las operaciones internas realizadas por el hardware son diferentes.

La motivación detrás de esta doble implementación es estudiar si dos realizaciones hardware distintas de un mismo esquema de modulación pueden generar patrones de consumo diferenciados. Este aspecto resulta particularmente relevante desde la perspectiva del análisis por canal lateral, ya que permitiría inferir no solo el tipo de modulación utilizado, sino también detalles relacionados con su implementación interna.

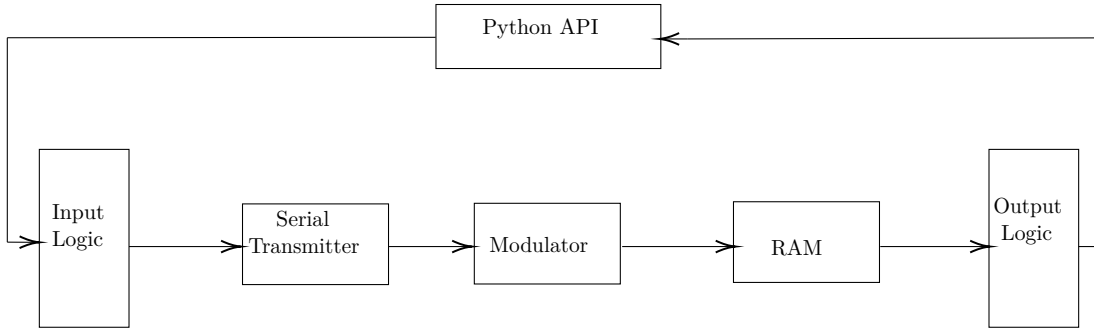


Figura 3.2: Modelo para la adquisición de datos.

La adquisición de potencia se inicia mediante una señal de disparo (*trigger*) generada cuando el transmisor serie comienza a enviar datos al bloque modulador. Esta señal permite alinear temporalmente la captura de las trazas con la ejecución del algoritmo, garantizando que todas las adquisiciones correspondan al mismo intervalo de procesamiento.

Cabe destacar que el análisis se centra exclusivamente en el transmisor. Aunque un sistema de comunicación completo incluye tanto transmisor como receptor, esta simplificación permite aislar el efecto de la modulación sobre el consumo de potencia y reducir la complejidad experimental sin comprometer los objetivos principales del estudio.

3.3. Caracterización y adquisición de potencia

Una vez implementada la arquitectura experimental, se procedió a la adquisición sistemática de trazas de potencia para cada esquema de modulación.

Las entradas utilizadas corresponden a secuencias aleatorias de símbolos generadas para cada ejecución experimental. La utilización de datos aleatorios busca evitar que las características extraídas dependan de patrones particulares de entrada. De esta manera, las diferencias observadas pueden asociarse principalmente al esquema de modulación y no a una secuencia específica de datos.

Se realizaron en total 10 experimentos para cada modulación y frecuencia. En cada experimento se procesaron 3072 símbolos de 8 bits. Estos símbolos fueron agrupados en bloques de 128 bits para su transmisión hacia la FPGA. Una vez recibidos todos los datos, el sistema ejecuta el proceso completo de modulación mientras se realiza simultáneamente la captura de potencia.

Con el objetivo de analizar el efecto de la frecuencia de operación sobre las trazas obtenidas, se evaluaron doce frecuencias distintas comprendidas entre 4 MHz y 26 MHz, utilizando incrementos de 2 MHz, lo que resulta en 12 frecuencias de reloj por experimento. Considerando lo anterior, en total se utilizaron 368 640 símbolos por modulación (10 experimentos $\times$ 3072 símbolos $\times$ 12 frecuencias).

La cantidad de muestras registradas en cada traza depende de la configuración de muestreo utilizada. En el caso de muestreo sincrónico, se consideraron dos escenarios: una muestra por ciclo de reloj y cuatro muestras por ciclo. Estas configuraciones corresponden a las opciones soportadas por la plataforma ChipWhisperer para captura sincronizada.

Por otra parte, para el muestreo asincrónico se utilizaron configuraciones equivalentes a dos y cuatro muestras por ciclo de reloj. En este caso se descartó la opción de una muestra por ciclo debido a la incertidumbre temporal inherente al muestreo asincrónico. Incrementar la frecuencia de adquisición permite compensar parcialmente esta limitación y mejorar la representación de la actividad interna del sistema.

Como resultado, se generaron cuatro conjuntos de datos diferentes que representan distintos escenarios de observación. Estos conjuntos permiten evaluar simultáneamente el impacto de la sincronización y de la frecuencia de muestreo sobre la capacidad de clasificación. Por la naturaleza del muestreo de cada conjunto, sus trazas presentan diferentes niveles de alineamiento temporal y resolución, lo que afecta la separabilidad entre clases.

3.4. Procesamiento y análisis de datos

Las trazas de potencia adquiridas contienen miles de muestras por observación. Utilizar directamente estas muestras como entrada de un clasificador incrementaría considerablemente la complejidad computacional y dificultaría la interpretación de los resultados. Por esta razón, se realizó una etapa previa de extracción de características.

El objetivo de esta etapa es resumir cada experimento mediante un conjunto reducido de parámetros capaces de capturar sus propiedades más relevantes. En este trabajo se seleccionaron los cuatro primeros momentos estadísticos: media, desviación estándar, asimetría y curtosis.

La media proporciona una estimación del nivel promedio de consumo energético. La desviación estándar mide la variabilidad de la señal y permite identificar diferencias en la actividad interna del circuito. La asimetría describe el grado de inclinación de la distribución de valores, mientras que la curtosis caracteriza la concentración de las muestras alrededor de la media y la presencia de valores extremos.

La elección de estas características se fundamenta en su simplicidad, interpretabilidad y bajo costo computacional. Además, permiten evaluar de forma directa si los distintos esquemas de modulación generan distribuciones de potencia significativamente diferentes.

Una vez obtenidas las características, se entrenaron modelos de clasificación utilizando el algoritmo XGBoost [18]. Este algoritmo se basa en técnicas de *gradient boosting* y combina múltiples árboles de decisión para construir un clasificador robusto capaz de modelar relaciones no lineales entre las variables de entrada.

Para el entrenamiento y la validación, se separó el conjunto de datos en una proporción 7:3. A partir de las características extraídas de cada experimento, se obtuvieron 120 vectores de características por modulación.

La evaluación de los modelos se realizó mediante las métricas de exactitud, precisión, exhaustividad y puntuación F1. Estas métricas proporcionan una visión complementaria del desempeño del clasificador, permitiendo analizar tanto su capacidad global de clasificación como el equilibrio entre falsos positivos y falsos negativos.

Finalmente, los resultados obtenidos permiten determinar si las características extraídas del consumo de potencia contienen información suficiente para identificar correctamente el esquema de modulación implementado. La validación de esta hipótesis constituye el objetivo principal de

la investigación y proporciona evidencia sobre la existencia de fugas de información explotables en sistemas de comunicación digital implementados sobre FPGA.

4 | Resultados

En este capítulo se presentan y analizan los resultados obtenidos durante el desarrollo experimental. El análisis se divide en dos etapas complementarias. En primer lugar, se estudian las características estadísticas extraídas de las trazas de consumo de potencia con el objetivo de determinar si existen diferencias observables entre los distintos esquemas de modulación implementados. Posteriormente, se evalúa el desempeño de los modelos de clasificación entrenados a partir de dichas características, permitiendo determinar hasta qué punto estas diferencias pueden ser explotadas de forma automática para identificar la modulación utilizada.

Más allá de cuantificar el rendimiento de los clasificadores, este análisis busca responder la pregunta central planteada en esta investigación: ¿contiene el consumo de potencia suficiente información para revelar el esquema de modulación implementado en un sistema digital?

4.1. Análisis estadístico

Antes de aplicar cualquier técnica de aprendizaje automático, resulta necesario verificar si las trazas de consumo de potencia contienen diferencias observables entre los distintos esquemas de modulación. Si tales diferencias no existieran, ningún clasificador podría aprender patrones discriminantes de forma fiable.

Con este propósito, se analizaron los primeros cuatro momentos estadísticos de las trazas adquiridas: media, desviación estándar, asimetría y curtosis. Estos parámetros permiten describir la distribución estadística de cada traza de manera compacta, capturando información relacionada con el nivel promedio de consumo, su variabilidad y la forma general de la distribución.

La Figura 4.1 muestra la evolución de estos cuatro momentos para los distintos esquemas de modulación bajo una configuración de muestreo sincrónico con una muestra por ciclo de reloj.

Una primera observación relevante es que los distintos esquemas de modulación no producen distribuciones estadísticas idénticas. Por el contrario, cada modulación presenta patrones relativamente consistentes a lo largo de las diferentes frecuencias de operación evaluadas. Este resultado constituye una primera evidencia de que las operaciones realizadas internamente por el modulador afectan de manera medible al consumo de potencia del dispositivo.

Desde un punto de vista físico, este comportamiento es coherente con el funcionamiento de los circuitos digitales descrito en el Capítulo 2. Diferentes esquemas de modulación requieren distintas secuencias de operaciones lógicas, accesos a memoria y conmutaciones internas. Dado

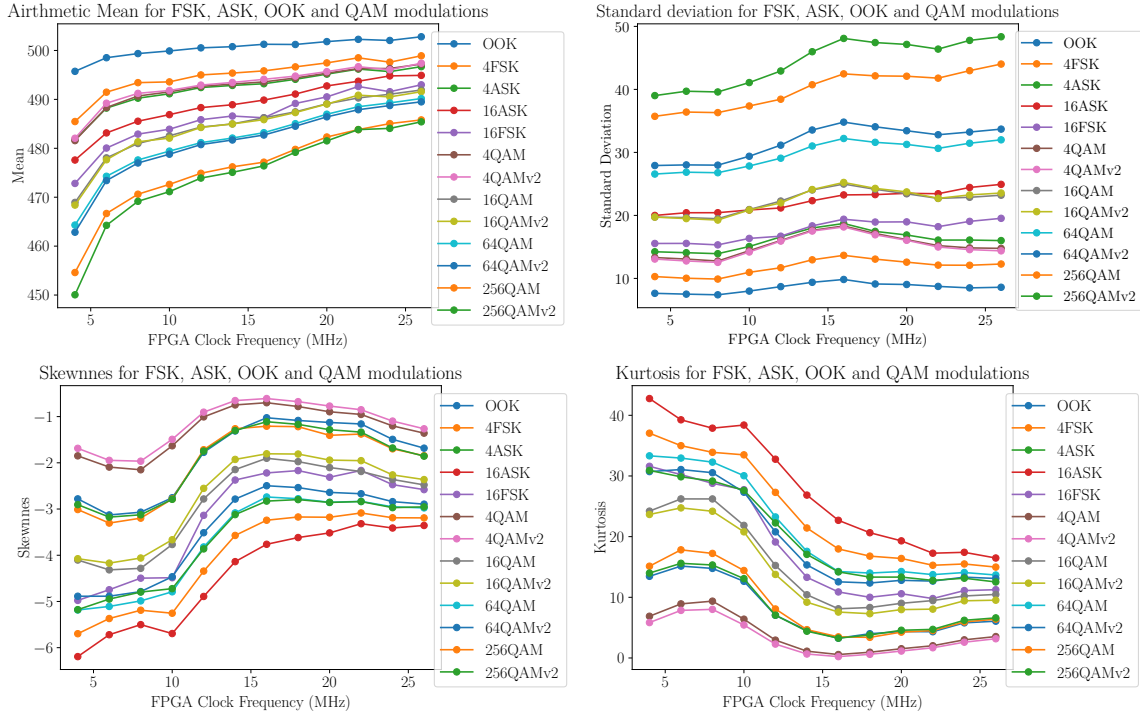


Figura 4.1: Media, desviación estándar, asimetría y curtosis para los distintos métodos de modulación con muestreo sincrónico a una muestra por ciclo de reloj.

que el consumo de potencia dinámica depende directamente de la actividad de los transistores, es esperable que modulaciones diferentes produzcan perfiles de consumo distintos.

Entre todas las características analizadas, la desviación estándar resulta particularmente ilustrativa. Esta métrica cuantifica la dispersión de los valores de potencia alrededor de su valor medio y, por tanto, puede interpretarse como una medida indirecta de la variabilidad de la actividad interna del circuito. La Figura 4.2 muestra este parámetro para el caso de muestreo asincrónico con dos muestras por ciclo de reloj.

Al comparar la Figura 4.2 con la Figura 4.1, puede observarse una diferencia importante entre los escenarios de muestreo sincrónico y asincrónico. En el caso sincrónico, los valores asociados a cada modulación presentan agrupaciones relativamente bien definidas, mientras que en el caso asincrónico se aprecia una dispersión considerablemente mayor.

Este comportamiento era esperable. Cuando la adquisición se encuentra sincronizada con el reloj de la FPGA, cada muestra captura aproximadamente el mismo instante del proceso de ejecución, reduciendo la variabilidad introducida por el sistema de medición. En cambio, durante el muestreo asincrónico, las muestras pueden corresponder a instantes ligeramente distintos de cada ciclo de reloj, introduciendo incertidumbre temporal que se manifiesta como ruido adicional en las trazas adquiridas.

A pesar de esta mayor dispersión, incluso en el caso asincrónico siguen observándose tendencias diferenciadas entre varios esquemas de modulación. Esto constituye un resultado relevante, ya que demuestra que la información característica del consumo de potencia no desaparece completamente cuando se pierde la sincronización, aunque sí se vuelve más difícil de explotar.

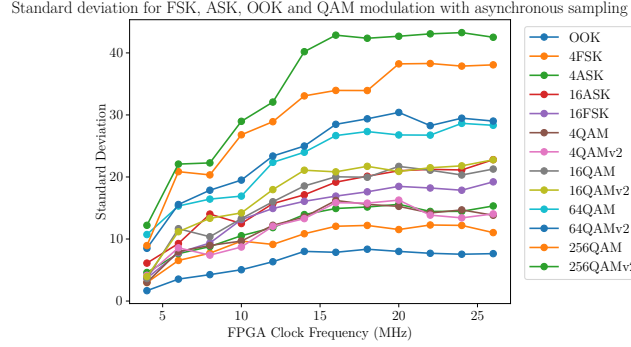


Figura 4.2: Desviación estándar para los distintos métodos de modulación con muestreo asincrónico a dos muestras por ciclo de reloj.

Por otra parte, la desviación estándar no es la única característica que aporta información útil. La media permite capturar diferencias en el nivel promedio de consumo energético, mientras que la asimetría y la curtosis describen aspectos más sutiles de la forma de la distribución. La asimetría indica si la distribución presenta una tendencia hacia valores superiores o inferiores al promedio, mientras que la curtosis proporciona información sobre la presencia de valores extremos o picos pronunciados.

Consideradas individualmente, estas métricas no siempre permiten separar completamente todas las modulaciones. Sin embargo, cuando se utilizan de forma conjunta, proporcionan una representación más completa del comportamiento estadístico de cada traza. Esta observación resulta especialmente importante, ya que constituye la base sobre la cual se construye posteriormente el modelo de clasificación.

En consecuencia, el análisis estadístico preliminar permite concluir que existen diferencias medibles y consistentes entre las trazas de potencia asociadas a los distintos esquemas de modulación. Aunque dichas diferencias no siempre son evidentes en una única característica, la combinación de múltiples descriptores estadísticos ofrece una representación suficientemente rica para justificar la aplicación de técnicas de aprendizaje automático.

4.2. Clasificación de esquemas de modulación

Una vez verificadas las diferencias estadísticas entre las trazas de potencia, se procedió a evaluar si dichas diferencias podían ser explotadas automáticamente mediante un algoritmo de clasificación.

Para ello se entrenaron modelos XGBoost utilizando como variables de entrada los cuatro momentos estadísticos previamente descritos. Se generó un modelo independiente para cada una de las configuraciones de adquisición consideradas, permitiendo comparar directamente el impacto del tipo de muestreo sobre el rendimiento de clasificación.

La Tabla 4.1 resume los resultados obtenidos.

Tabla 4.1: Rendimiento de los modelos de clasificación

Conjunto de datos	Exactitud	Exhaustividad	Precisión	Punt. F1
Muestreo asincrónico 2x	0.77	0.77	0.78	0.751
Muestreo asincrónico 4x	0.87	0.87	0.87	0.865
Muestreo sincrónico 1x	0.98	0.98	0.98	0.982
Muestreo sincrónico 4x	0.99	0.99	0.99	0.989

Los resultados muestran una diferencia clara entre los escenarios de adquisición sincronizada y no sincronizada. El modelo de menor rendimiento corresponde al caso de muestreo asincrónico con dos muestras por ciclo, donde la exactitud alcanza un 77 %.

La matriz de confusión correspondiente, presentada en la Figura 4.3a, permite identificar con mayor detalle el origen de los errores de clasificación.

En este escenario se observa que algunas modulaciones son clasificadas correctamente con elevada frecuencia, mientras que otras presentan confusiones recurrentes. En particular, aparecen errores entre modulaciones de orden similar, como 16-FSK y 16-QAM, así como entre distintas modulaciones de bajo orden. Este comportamiento es consistente con el análisis estadístico realizado anteriormente, donde ya se observaban regiones de solapamiento entre algunas clases.

Cuando el número de muestras aumenta a cuatro muestras por ciclo de reloj, el rendimiento mejora significativamente, alcanzando una exactitud cercana al 87 %. Este resultado indica que una mayor resolución temporal permite capturar con mayor precisión las variaciones del consumo de potencia, compensando parcialmente la pérdida de información causada por la ausencia de sincronización.

Los mejores resultados se obtienen en los escenarios de muestreo sincrónico. Incluso utilizando únicamente una muestra por ciclo de reloj, el clasificador alcanza una exactitud cercana al 98 %. Al aumentar la resolución temporal a cuatro muestras por ciclo, el rendimiento se aproxima al 99 %.

Este resultado es particularmente interesante porque demuestra que la sincronización temporal tiene un impacto mucho mayor que el incremento de la frecuencia de muestreo. En otras palabras, capturar las muestras en el instante correcto resulta más importante que aumentar simplemente la cantidad de muestras adquiridas.

Asimismo, las matrices de confusión muestran que el modelo es capaz de distinguir correctamente modulaciones pertenecientes a una misma familia e incluso modulaciones con igual orden. Este comportamiento sugiere que las diferencias observadas no se limitan únicamente al número de símbolos de la constelación, sino que reflejan características más profundas relacionadas con la implementación hardware de cada modulador.

4.3. Discusión de los resultados

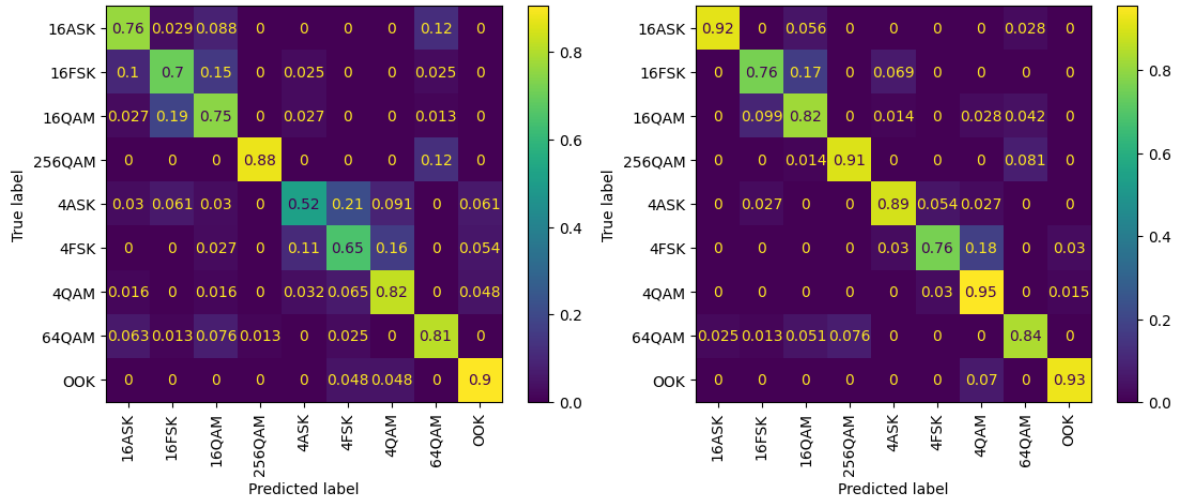
Los resultados obtenidos permiten validar la hipótesis planteada al inicio de este trabajo: el consumo de potencia contiene información suficiente para identificar esquemas de modulación digital implementados en una FPGA.

Uno de los hallazgos más relevantes es que esta información puede extraerse utilizando únicamente características estadísticas simples. A diferencia de muchos enfoques de análisis de señales que requieren transformaciones complejas o modelos profundos de aprendizaje automático, en este caso cuatro descriptores estadísticos resultan suficientes para alcanzar niveles de exactitud cercanos al 99 %.

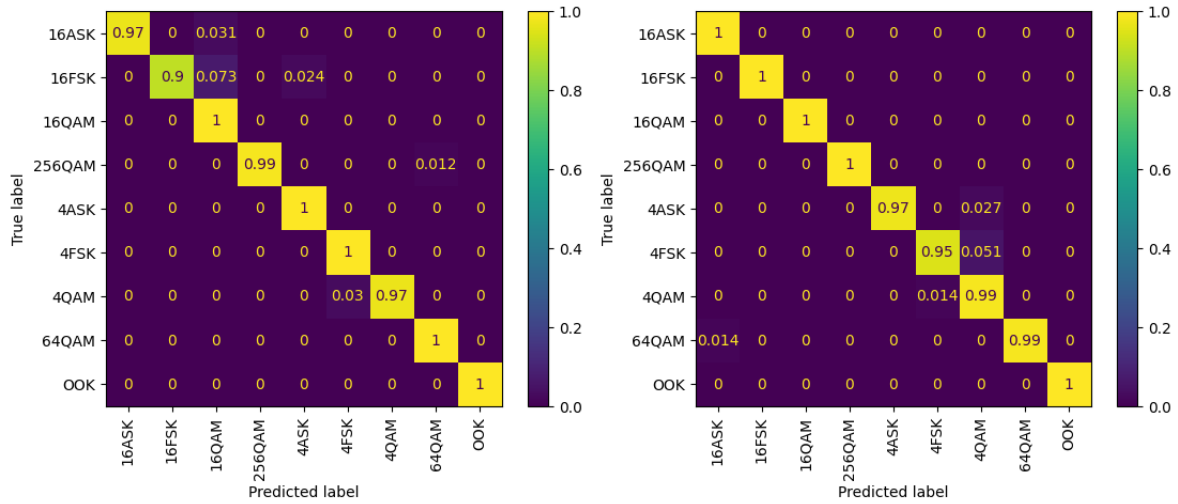
Otro aspecto destacable es la influencia de la sincronización sobre el rendimiento del sistema. La diferencia observada entre los escenarios sincrónicos y asincrónicos confirma la importancia del alineamiento temporal en los ataques por canal lateral. Sin embargo, incluso en el escenario más desfavorable considerado, el clasificador mantiene una exactitud superior al 75 %, lo que demuestra que la fuga de información sigue siendo explotable aun cuando las condiciones de adquisición no son ideales.

Desde una perspectiva de seguridad, estos resultados sugieren que los esquemas de modulación implementados en hardware pueden revelar información sensible a través de su consumo de potencia. Aunque el presente trabajo no busca desarrollar un ataque práctico contra sistemas reales, sí demuestra la existencia de un canal de información potencialmente explotable.

Finalmente, si bien los resultados obtenidos son comparables a los alcanzados por algunos sistemas tradicionales de clasificación de modulación en condiciones favorables de SNR, ambos enfoques operan sobre fuentes de información completamente distintas. Por esta razón, más que considerarse una alternativa directa a la Clasificación Automática de Modulación convencional, el método propuesto puede entenderse como una fuente complementaria de información que podría combinarse con técnicas tradicionales para mejorar la capacidad de identificación de sistemas de comunicación digital.



(a) Muestreo asincrónico con dos muestras por ciclo de reloj. (b) Muestreo asincrónico con cuatro muestras por ciclo de reloj.



(c) Muestreo sincrónico con una muestra por ciclo de reloj. (d) Muestreo sincrónico con cuatro muestras por ciclo de reloj.

Figura 4.3: Matrices de confusión para la clasificación de modulaciones mediante XGBoost en los distintos escenarios de adquisición.

5 | Conclusiones

El objetivo principal de este trabajo fue investigar si el consumo de potencia de un sistema digital contiene información suficiente para identificar el esquema de modulación implementado. Para ello, se desarrolló una plataforma experimental basada en FPGA que permitió implementar distintos moduladores digitales, adquirir trazas de consumo de potencia bajo diferentes condiciones de operación y evaluar la capacidad de un modelo de aprendizaje automático para distinguir entre ellos.

Los resultados obtenidos permiten responder afirmativamente a esta pregunta. A lo largo del estudio se demostró que diferentes esquemas de modulación generan patrones de consumo de potencia distinguibles, incluso cuando se ejecutan sobre una misma plataforma hardware y procesan datos aleatorios. Mediante la extracción de características estadísticas simples y el uso de un clasificador basado en XGBoost, fue posible identificar correctamente la modulación utilizada con niveles de exactitud que alcanzan aproximadamente un 99 % en los escenarios de muestreo sincrónico.

Más allá de la elevada precisión obtenida, uno de los hallazgos más relevantes de esta investigación es la confirmación de que el proceso de modulación deja una huella observable en el comportamiento eléctrico del sistema. Este resultado demuestra que el consumo de potencia puede actuar como una fuente alternativa de información para inferir características internas de un transceptor, incluso sin necesidad de analizar directamente la señal de radiofrecuencia transmitida.

Asimismo, los resultados evidencian la influencia crítica del proceso de adquisición sobre el rendimiento del análisis. En particular, el muestreo sincrónico permitió capturar de forma más precisa la actividad interna de la FPGA, obteniendo los mejores resultados de clasificación. Sin embargo, incluso en escenarios asincrónicos, donde la adquisición se realiza sin alineamiento temporal con el reloj del sistema, el modelo mantuvo niveles de rendimiento elevados. Esto sugiere que la fuga de información observada es suficientemente robusta como para seguir siendo explotable bajo condiciones menos favorables y potencialmente más cercanas a aplicaciones reales.

Desde una perspectiva más amplia, este trabajo contribuye a extender el alcance tradicional del análisis por canal lateral. Históricamente, estas técnicas han sido estudiadas principalmente en el contexto de la criptografía, donde se utilizan para recuperar claves secretas u otra información sensible. Los resultados obtenidos muestran que conceptos similares pueden aplicarse también al ámbito de las comunicaciones digitales, permitiendo inferir parámetros de funcionamiento de un sistema a partir de sus características físicas de operación.

No obstante, el presente estudio constituye una primera aproximación al problema y presenta

ciertas limitaciones. En primer lugar, el análisis se ha centrado exclusivamente en el transmisor, sin considerar el comportamiento de un sistema completo de comunicación. Asimismo, las mediciones se realizaron en un entorno controlado y con acceso directo a la alimentación del dispositivo, una condición que no siempre estará disponible en escenarios prácticos. Finalmente, la representación de las trazas se basó únicamente en momentos estadísticos, sin explorar métodos más avanzados de extracción de características.

Estas limitaciones abren diversas líneas de investigación futura. Una extensión natural consiste en analizar sistemas de comunicación más complejos, incorporando receptores y arquitecturas de procesamiento más sofisticadas. Del mismo modo, sería interesante estudiar el uso de técnicas avanzadas de procesamiento de señales y aprendizaje automático, incluyendo representaciones en frecuencia, métodos de reducción de dimensionalidad o modelos basados en aprendizaje profundo. Otra dirección prometedora es la combinación de información proveniente de múltiples fuentes, integrando datos de canal lateral con observaciones de radiofrecuencia para construir sistemas de clasificación más robustos.

Finalmente, también resulta de interés explorar otros canales laterales menos invasivos, como las emisiones electromagnéticas, que podrían permitir la obtención de información sin necesidad de acceder físicamente a las líneas de alimentación del dispositivo. Este tipo de estudios contribuiría a comprender mejor las vulnerabilidades potenciales de los sistemas de comunicación modernos y las medidas necesarias para mitigarlas.

En síntesis, este trabajo demuestra que el consumo de potencia constituye una fuente de información rica y explotable para la identificación de esquemas de modulación digital. Los resultados obtenidos validan la hipótesis planteada inicialmente y ponen de manifiesto la existencia de una fuga de información previamente poco explorada en el ámbito de las comunicaciones digitales. De esta manera, la investigación abre nuevas posibilidades tanto para la ingeniería inversa de sistemas inalámbricos como para el estudio de mecanismos de protección frente a ataques por canal lateral en futuras generaciones de dispositivos de comunicación.

Bibliografía

- [1] P. Pareja, Y. Nasser, A. Masmoudi, and S. Houcke, “Power consumption analysis for reverse engineering digital modulation: A novel approach to physical layer attacks on communication systems,” in *Cybersecurity* (I. Praça, S. Bernardi, and P. R. Inácio, eds.), (Cham), pp. 52–62, Springer Nature Switzerland, 2025.
- [2] Z. Zhu and A. K. Nandi, *Automatic modulation classification: principles, algorithms, and applications*. Hoboken: John Wiley & Sons Inc, 2015.
- [3] B. Yalcinkaya, R. B. Coruk, A. Kara, and H. Tora, “Hierarchical Classification of Analog and Digital Modulation Schemes Using Higher-Order Statistics and Support Vector Machines,” *Wireless Personal Communications*, vol. 136, pp. 827–847, May 2024.
- [4] P. Ghasemzadeh, S. Banerjee, M. Hempel, and H. Sharif, “Accuracy analysis of feature-based automatic modulation classification with blind modulation detection,” in *2019 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1000–1004, 2019.
- [5] Y. Nasser, C. Sau, J.-C. Prévotet, T. Fanni, F. Palumbo, M. H  lard, and L. Raffo, “Neupow: A cad methodology for high-level power estimation based on machine learning,” *ACM Trans. Des. Autom. Electron. Syst.*, vol. 25, aug 2020.
- [6] J. Lorandel, J.-C. Pr  votet, and M. H  lard, “Fast power and performance evaluation of fpga-based wireless communication systems,” *IEEE Access*, vol. 4, pp. 2005–2018, 2016.
- [7] B. Sklar, *Digital Communications: Fundamentals and Applications*. Prentice Hall, 2 ed., 2001. ISBN-10: 0130847887. Publication date: 24 Jan. 2001.
- [8] T. Huynh-The, Q.-V. Pham, T.-V. Nguyen, T. T. Nguyen, R. Ruby, M. Zeng, and D.-S. Kim, “Automatic modulation classification: A deep architecture survey,” *IEEE Access*, vol. 9, pp. 142950–142971, 2021.
- [9] S. Huang, C. Lin, K. Zhou, Y. Yao, H. Lu, and F. Zhu, “Identifying physical-layer attacks for iot security: An automatic modulation classification approach using multi-module fusion neural network,” *Physical Communication*, vol. 43, p. 101180, 2020.
- [10] W. Shi, X. Jiang, J. Hu, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu, and J. Wang, “Physical layer security techniques for future wireless networks,” 2021.
- [11] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, “Systematic classification of side-channel attacks: A case study for mobile devices,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 465–488, 2018.

- [12] M. Randolph and W. Diehl, “Power side-channel attack analysis: A review of 20 years of study for the layman,” *Cryptography*, vol. 4, no. 2, 2020.
- [13] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, “Machine learning in side-channel analysis: a first study,” *Journal of Cryptographic Engineering*, vol. 1, pp. 293–302, Dec. 2011.
- [14] B. Hettwer, S. Gehrler, and T. Güneysu, “Applications of machine learning techniques in side-channel attacks: a survey,” *Journal of Cryptographic Engineering*, vol. 10, pp. 135–162, June 2020.
- [15] C. O’Flynn and Z. D. Chen, “Chipwhisperer: An open-source platform for hardware embedded security research,” in *Constructive Side-Channel Analysis and Secure Design* (E. Prouff, ed.), (Cham), pp. 243–260, Springer International Publishing, 2014.
- [16] C. O’Flynn and Z. Chen, “Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection,” *Journal of Cryptographic Engineering*, vol. 5, pp. 53–69, Apr. 2015.
- [17] N. T. Inc., “Chipwhisperer.” <https://github.com/newaetech/chipwhisperer>, 2024.
- [18] T. Chen and C. Guestrin, “XGBoost: A Scalable Tree Boosting System,” 2016.