Universidad de Valencia



**Texto

Descripción generada automáticamente**

**Grado en Ingeniería Electrónica Industrial**

Trabajo de Fin de Grado

**Seguridad en Microcontroladores:**

**Análisis de Side-Channel Attacks y Contramedidas.**

**Autor: ABDALAH EL KENNOUSSI**

**Tutor: José Rafael Lajara**

**Valencia, Octubre – 2023**

# DECLARACION DE AUTORÍA

**Yo, ABDALAH EL KENNOUSSI declaro la autoría del Trabajo Fin de Grado titulado “Seguridad en Microcontroladores: Análisis de Side-Channel Attacks y Contramedidas” y que el citado trabajo no infringe las leyes en vigor sobre propiedad intelectual. El material no original que figura en este trabajo ha sido atribuido a sus legítimos autores.**

**Valencia, 1 de enero de 2023**

**Fdo:**

# RESUMEN

En los microcontroladores existen diversos tipos de ataques. Algunos se pueden clasificar como directos y hacen operaciones como un volcado de memoria por JTAG. Otros buscan mecanismos indirectos, son los side-channel attacks.

En este proyecto haremos el estudio de dos tipos de ataques indirectos y propondremos unas contramedidas para evitarlos. Nos centraremos en el “Power Analysis” y “Clock Glitching” que generalmente son los ataques más conocidos por su eficacia a la hora de deducir contraseñas y códigos encriptados.

El primer paso es estudiar el funcionamiento del sistema “CHIPWHISPERER LITE” y entender su funcionamiento con los dos tipos de ataques. A partir de aquí se planteará y ejecutarán los dos tipos de ataques para ver cómo reacciona nuestro Target, que en este caso es el ARM CORTEX-M.

Una vez realizados los ataques y obtenidos los resultados se procederá a realizar un estudio de prevención en contra de los dos tipos de ataques y se pondrán a prueba para ver si surquen efecto.

# AGRADECIMIENTOS

Quiero expresar mi sincero agradecimiento a todos los profesores por el apoyo y el gran trabajo y conocimientos aportados durante la carrera, pero en especial a José Rafael Lajara que ha sido mi tutor y apoyo durante la realización de este trabajo de fin de grado. Su experiencia y conocimientos en este sector me han servido de guía durante todo el proceso de investigación y redacción de mi tesis. Su compromiso con la excelencia académica y su disposición a invertir tiempo y esfuerzo en este proyecto me han ayudado a mejorar muchas cualidades en este sector y cada vez interesarme más.

Además, quiero agradecerle por su paciencia y disponibilidad para responder a mis preguntas, aclarar mis dudas y ofrecer sugerencias constructivas que han mejorado significativamente este proyecto.

Espero tener la oportunidad de mantener el contacto y continuar aprendiendo de usted en el futuro. Gracias una vez más por su apoyo inquebrantable.

# Contents

[1 DECLARACION DE AUTORÍA 2](#_Toc150459740)

[2 RESUMEN 3](#_Toc150459741)

[3 AGRADECIMIENTOS 5](#_Toc150459742)

[4 ÍNDICE 7](#_Toc150459743)

[5 Contents 7](#_Toc150459744)

[6 Introcucción 9](#_Toc150459745)

[6.1 Introducción 9](#_Toc150459746)

[6.2 Motivación 10](#_Toc150459747)

[6.3 Objetivos 11](#_Toc150459748)

[7 Materiales y métodos 13](#_Toc150459749)

[7.1 ChipWhiperer Lite 32 Bits con Target Device Incorporado 13](#_Toc150459750)

[7.2 Máquina Virtual de ChipWhisperer 17](#_Toc150459751)

[7.3 CHIPWHISPERER LITE 17](#_Toc150459752)

[7.4 CHIPWHISPERER HUSKY 17](#_Toc150459753)

[7.5 TIPOS DE TARGETS 17](#_Toc150459754)

[8 ESTUDIO TEÓRICO 19](#_Toc150459755)

[8.1 TIPOS DE SIDE CHANNEL ATTACKS 19](#_Toc150459756)

[8.2 POWER ANALYIS ATTACK 19](#_Toc150459757)

[8.3 POSIBLE CONTRAMEDIDA DEL POWER ANALYSIS ATTACK 19](#_Toc150459758)

[8.4 CLOCK GLITCHING ATTACK 19](#_Toc150459759)

[8.5 POSIBLE CONTRAMEDIDA DEL CLOCK GLITCHING ATTACK 19](#_Toc150459760)

[9 ESTUDIO EXPERIMENTAL 21](#_Toc150459761)

[9.1 PRUEBAS INICIALES EN EL CHIPWHISPERER LITE 32BITS 21](#_Toc150459762)

[9.2 PRUEBAS INICIALES EN EL TARGET ARM CORTEX – M 21](#_Toc150459763)

[9.3 POWER ANALYSIS ATTACK SIMULACION 21](#_Toc150459764)

[9.4 ANÁLISIS DE RESULTADOS 21](#_Toc150459765)

[9.5 PRUEBA DE LA CONTRAMEDIDA CONTRA EL ATAQUE 21](#_Toc150459766)

[9.6 RESULTADOS Y CONCLUSIÓN 21](#_Toc150459767)

[9.7 CLOCK GLITCHING ATTACK SIMULACIÓN. 21](#_Toc150459768)

[9.8 ANÁLISIS DE RESULTADOS 21](#_Toc150459769)

[9.9 PRUEBA DE LA CONTRAMEDIDAD CON EL ATAQUE 21](#_Toc150459770)

[10 RESULTADOS Y CONCLUSIÓN 21](#_Toc150459771)

[11 CONCLUSIONES 23](#_Toc150459772)

[12 APÉNDICES 25](#_Toc150459773)

[13 BIBLIOGRAFÍA 27](#_Toc150459774)

# Introcucción

## Introducción

Los *Side Channel Attacks* son un tipo de ataque informático que explora las fugas involuntarias de información que se producen durante el funcionamiento de un sistema, un ordenador o cualquier dispositivo electrónico. A diferencia de los ataques tradicionales que se centran en vulnerabilidades en el software o hardware, este tipo de ataques se basan en la observación de señales indirectas o canales colaterales, como el consumo de energía, el tiempo de ejecución o las emisiones electromagnéticas para descifrar información encriptada.

Estos ataques pueden tener como objetivo la obtención de datos confidenciales, como claves de cifrado, contraseñas o información personal, sin acceder directamente a la fuente de esos datos. Los *Side Channel Attacks* pueden ser especialmente peligrosos en entornos donde la seguridad de la información es crítica, como sistemas de criptografía, sistemas de pago electrónico o dispositivos médicos.

Los investigadores y expertos en ciberseguridad trabajan constantemente en la detección y mitigación de los *Side Channel Attacks*, desarrollando técnicas de contramedidas, como el enmascaramiento de datos, la introducción de ruido en las señales o el diseño de hardware resistente a este tipo de ataques. La comprensión de las amenazas asociadas a estos ataques es esencial para garantizar la integridad y la confidencialidad de los sistemas y datos en un mundo cada vez más conectado y dependiente de la tecnología.

En general, los ataques por canales laterales se aprovechan de la implementación hardware de un sistema informático en algoritmos como el *Advanced Encrypton Standard* (AES) o el *Triple Data Ecryption Algorithm* (DEA) para explotarlos por medio de diferentes ataques laterales.

## Motivación

Investigar el tema de los *Side Channel Attacks* es fundamental en el mundo actual de la ciberseguridad. Estas amenazas, que se basan en el análisis de información indirecta, representan un desafío constante y una oportunidad de mejora en la protección de datos y sistemas.

En la era digital en la que vivimos, la información es el recurso más valioso. La seguridad de esta información es esencial para proteger nuestras vidas, nuestra privacidad y nuestras instituciones. En este contexto, la investigación de los *Side Channel Attacks* se vuelve una tarea crítica.

Al comprender en profundidad cómo funcionan los *Side Channel Attacks* podemos desarrollar contramedidas efectivas para prevenirlos y proteger nuestros sistemas y datos. La investigación en esta área nos permite anticiparnos a los posibles agresores y fortalecer nuestras defensas.

Además, la investigación en *Side Channel Attacks* fomenta la innovación en la seguridad cibernética. A medida que los atacantes desarrollan nuevas técnicas, los investigadores también deben estar un paso adelante, diseñando sistemas más robustos y seguros. Esta constante competencia es lo que impulsa el avance de la tecnología y nos permite mantenernos a salvo en un mundo cada vez más interconectado.

En resumen, la investigación en *Side Channel Attacks* es crucial porque nos ayuda a proteger nuestra información, promueve la innovación en seguridad cibernética y puede tener un impacto positivo en muchas áreas de la tecnología. Al trabajar juntos para comprender y mitigar estas amenazas, podemos garantizar un futuro digital más seguro y confiable. Se espera que este trabajo sirva como base para otros futuros trabajos de investigación que avancen en nuevos conocimientos de este tipo de ataques y contramedidas en nuevos *targets*.

## Objetivos

En este TFG nuestro objetivo es estudiar 2 tipos de ataques laterales: El *Power Analysis Attack* y el *Clock Glitching*.

Para este estudio emplearemos el hardware CHIPWHISPERER LITE y nuestro Target víctima será un ARM CORTEX – M.

El objetivo principal es realizar los dos ataques utilizando nuestro micro y ver cómo reacciona nuestro Target. Una vez obtenidos los resultados se estará en condiciones de proponer contramedidas y ponerlas a prueba para evitar este tipo de brechas.

[PENSAR QUE MAS OBJETIVOS PONER XD PORQUE ESTA VACÍO…]

Estudiar programas susceptibles a ataques

Desarrollar programas que incluyan contramedidas

# Materiales y métodos

## ChipWhiperer Lite 32 Bits con Target Device Incorporado

El ChipWhisperer-Lite representa la búsqueda más agresiva de NewAE Technology Inc. para proporcionar de la forma más fácil y eficaz el estudio de los ataques laterales, tanto los ataques de potencia como los ataques de Glitching de reloj a cualquier persona con conocimientos en el sector, de estudiantes a ingenieros de software. Es completamente de código abierto (hardware, software, firmware, código FPGA) y está proporcionando una revolución en la seguridad de hardware.

El ChipWhisperer-Lite integra hardware para realizar mediciones de análisis de potencia, programación de dispositivos, Glitching, comunicaciones serie y un ejemplo de objetivo que puede cargarse con algoritmos criptográficos, todo en una sola placa. La versión de placa única viene en dos variantes: Atmel XMEGA o STM32F3 como objetivo víctima.

Se puede separar la parte de captura y el *target* para conectarlos a otros objetivos. La parte de captura está disponible como un componente independiente y viene lista con conectores SMA y para el objetivo, pero requiere un objetivo externo.

**Especificaciones:**

**Tabla

Descripción generada automáticamente**

Estas son las especificaciones que adjunta nuestra placa y podemos observar que en este caso los dos tipos de ataques disponibles son el de reloj y el de la potencia. Por otra parte, se puede observar cual es nuestro Target Device o víctima, que varía según el tipo de placa, pero en esta en concreto nos ofrecen el STM32Fx.

Por otra parte, se pueden observar los tiempos de medida que ofrece la placa con un Offset de 200 ps como mínimo. Tiene rangos de frecuencia de 5 a 200 MHz y una salida de reloj con salida de glitch incorporada.

Tipo de ataque de potencia tanto de alta tensión como de baja tensión con un pulso de corriente de 20A.

**Arquitectura síncrona:**

**Imagen de la pantalla de una computadora

Descripción generada automáticamente con confianza media**

ChipWhisperer puede utilizar el reloj de un dispositivo objetivo y aplicar multiplicaciones y desplazamientos de fase para muestrear en el punto deseado(s) durante el ciclo de reloj. Esto asegura que los puntos de muestreo estén directamente relacionados con el reloj digital que genera las señales de interés. El resultado es que muchos dispositivos pueden ser atacados con una frecuencia de muestreo de 5 a 100 veces más lenta en comparación con un osciloscopio regular.

**Tipos de placa:**

Un circuito electrónico

Descripción generada automáticamente con confianza media

La compañía ofrece varias posibilidades a la hora de realizar la compra. En esta imagen se puede observar la parte de captura y el objetivo en una misma placa, pero cabe la posibilidad de realizar la compra por partes separadas si el objetivo que queremos atacar es diferente o si queremos incorporar osciloscopios externos u otros tipos de medidores.

En las siguientes imágenes podemos observar los diferentes tipos de pedidos que se pueden realizar:

Tipo 1:

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Este modelo es con el cual vamos a trabajar. Incorpora en la misma placa el objetivo y la placa de medida, todo interconectado entre sí. Es más útil si se tiene claro el tipo de ataques que se quieren realizar y el objetivo deseado, aunque te limita el acceso a otras funciones.

Tipo 2:

Texto

Descripción generada automáticamente

Este modelo solo incorpora la parte de captura por lo que se necesitaría comprar aparte un objetivo para atacar. Por eso incorpora cables y conectores para poder realizar las medidas y las conexiones necesarias.

Tipo 3:

Interfaz de usuario gráfica, Sitio web

Descripción generada automáticamente

Este modelo incorpora las dos partes anteriores, pero por separado. Es decir, tanto la placa de captura como el objetivo, pero en diferentes placas además de aportar cables de conexionado para poder interconectarlo todo.

En resumen, dependiendo del tipo de pruebas que se quieran realizar y el nivel de conocimiento que se tenga, se elige un tipo o el otro.

**Software:**

El Chipwhisperer ofrece un software incorporado que te permite realizar todo tipo de medidas y programación necesaria. ChipWhisperer es una cadena de herramientas de código abierto para la investigación en seguridad embebida. Todas las metas y el hardware de captura en este catálogo son compatibles con una aplicación de captura basada en Python. La naturaleza de código abierto significa que se pueden realizar modificaciones según necesidades específicas, ya sea desarrollando tus propios algoritmos o realizando validaciones en objetivos propietarios.

Interfaz de usuario gráfica

Descripción generada automáticamente

## Máquina Virtual de ChipWhisperer

Hay varias formas de realizar la instalación de todo lo necesario para poder ejecutar todas las funciones del Micro, pero existe la posibilidad de descargar la máquina virtual en la cual está incorporado todas las funciones y programas de captura y ataque para el ChipWhisperer.

En este TFG, trabajaremos con VirtualBox y la extensión o la imagen de la computadora preconfigurada del ChipWhisperer.

## CHIPWHISPERER LITE

## CHIPWHISPERER HUSKY

## TIPOS DE TARGETS

# ESTUDIO TEÓRICO

## TIPOS DE SIDE CHANNEL ATTACKS

## POWER ANALYIS ATTACK

## POSIBLE CONTRAMEDIDA DEL POWER ANALYSIS ATTACK

## CLOCK GLITCHING ATTACK

## POSIBLE CONTRAMEDIDA DEL CLOCK GLITCHING ATTACK

# ESTUDIO EXPERIMENTAL

## PRUEBAS INICIALES EN EL CHIPWHISPERER LITE 32BITS

## PRUEBAS INICIALES EN EL TARGET ARM CORTEX – M

## POWER ANALYSIS ATTACK SIMULACION

## ANÁLISIS DE RESULTADOS

## PRUEBA DE LA CONTRAMEDIDA CONTRA EL ATAQUE

## RESULTADOS Y CONCLUSIÓN

## CLOCK GLITCHING ATTACK SIMULACIÓN.

## ANÁLISIS DE RESULTADOS

## PRUEBA DE LA CONTRAMEDIDAD CON EL ATAQUE

# RESULTADOS Y CONCLUSIÓN

# CONCLUSIONES

# APÉNDICES

# BIBLIOGRAFÍA