J ♣

Step 1-A
Start

Welcome to ChipWhisperer®!

To play along you'll need the following:

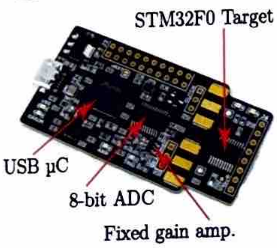
CW-Lite || CW-Nano || CW-Husky

+

Your computer.

Q ♣

Step 1-B
Nano

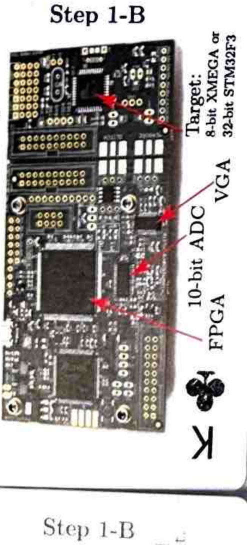


The CW-Nano is designed as a teaching platform for working primarily with the included target.

K ♣

Step 1-B

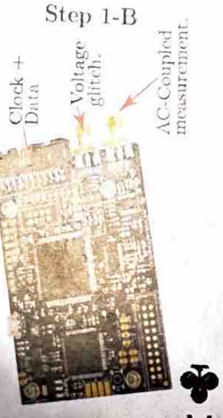
Lite (XMEGA/32-bit)



A ♣

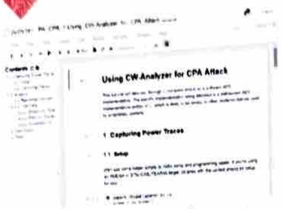
Step 1-B

Lite Capture



J ♥

Step 2-A
Jupyter



Using CW-Analyzer for CPA Attack

1 Capturing Power Traces

1.1 Setup

The best experience is now with ChipWhisperer 5, which uses Jupyter notebooks. These are interactive Python notebooks, allowing you to explore power analysis and fault injection.

Q ♥

Step 2-B
Virtual Machine

The quickest method of getting started is with a Virtual Machine using VirtualBox. This runs as a server on your computer, which you access via your web-browser. You need to configure a password the first time you run this. See the "releases" tab at:

https://github.com/newaetech/chipwhisperer

K ♥

Step 2-B
Windows Installer

You can run the Jupyter server natively as well. A simple Windows installer provides the required packages including the compiler for the target device. The installer can be found on the releases page.

A ♥

Step 2-B
Linux/Mac Installation

A full install can be made on Linux or Mac from your preferred package repositories. You'll need to begin by installing:

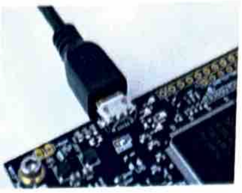
python3 python3-pip python3-tk
avr-libc gcc-avr gcc-arm-none-eabi

The remaining packages (including Jupyter) will be installed by following the requirements file.

See the full documentation for complete details of this.

J ♠

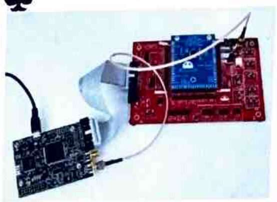
Step 3-A
USB



The CW-Nano and CW-Lite only need the USB cable connected. A blinking LED indicates the USB driver has loaded OK.

Q ♠

Step 3-B
Capture



The stand-alone capture board requires a connection to the target board:

1. Use 20-pin cable for power, data, and clock.
2. Use SMA for power measurement (or glitch out).

K ♠

Step 3-C
UFO

If using the UFO target baseboard, mount a target onto it and:

1. Enable VCC supplies as required by specific target.
2. Ensure clock jumpers correct.
3. Connect external programmer (if required).

A ♠

Step 3-D
20-Pin

ChipWhisperer®

1	2
+5V	GND
+3.3V	HS1/I
nRST	HS2/O
MISO	VREF
MOSI	IO1
SCK	IO2
PC	IO3
PD	IO4
GND	+3.3V
GND	+5V
19	20

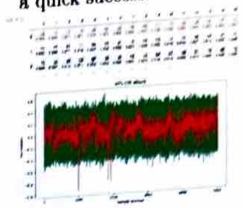
Connector View

This card has the pinout of the 20-pin cable. This can be useful to break out the individual signals.

J ♦

Step 4-A
AES Attack

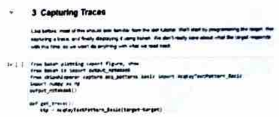
Tutorial "Lab 4_2 - CPA on Firmware Implementation of AES" will introduce you to attacking AES, and give you a quick success!



Q ♦

Step 4-B
SPA

Tutorial "Lab 2_1B - Power Analysis for Password Bypass" will introduce you to power analys in more general terms.



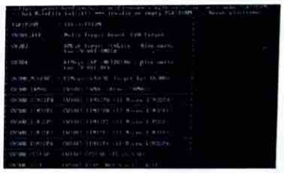
3 Capturing Traces

```
from bokeh.plotting import figure, show
from bokeh.io import output_notebook
[illegible]
import numpy as np
output_notebook()

def get_trace():
    [illegible]
```

K ♦

Step 4-C
Porting



The ChipWhisperer firmware examples include an extensive build system allowing you to port new code to any of the targets.

A ♦

Step 4-D
Glitching

The ChipWhisperer-{Lite, Pro, Husky} demonstrate glitching for dumping memory, fault attacks on AES and RSA, and more. The Lite and Pro can perform both VCC and clock glitching.

A subset of the VCC glitch attack demos can also be performed on the Nano.