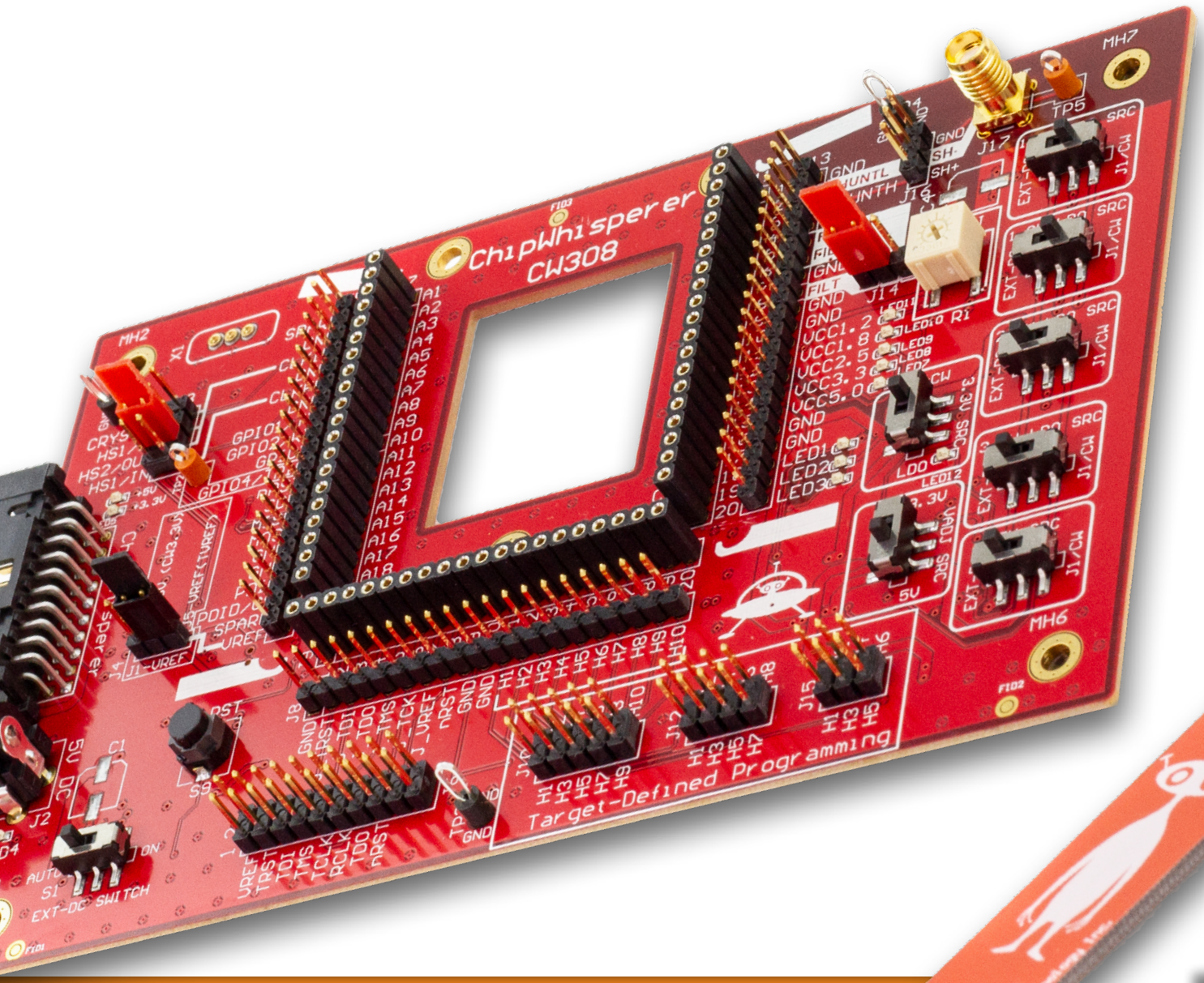
FALL 2020

NewAE Technology

NewAE

Your friendly embedded security arsonist

Tools, Training and information on advanced embedded security attacks



CONTENT

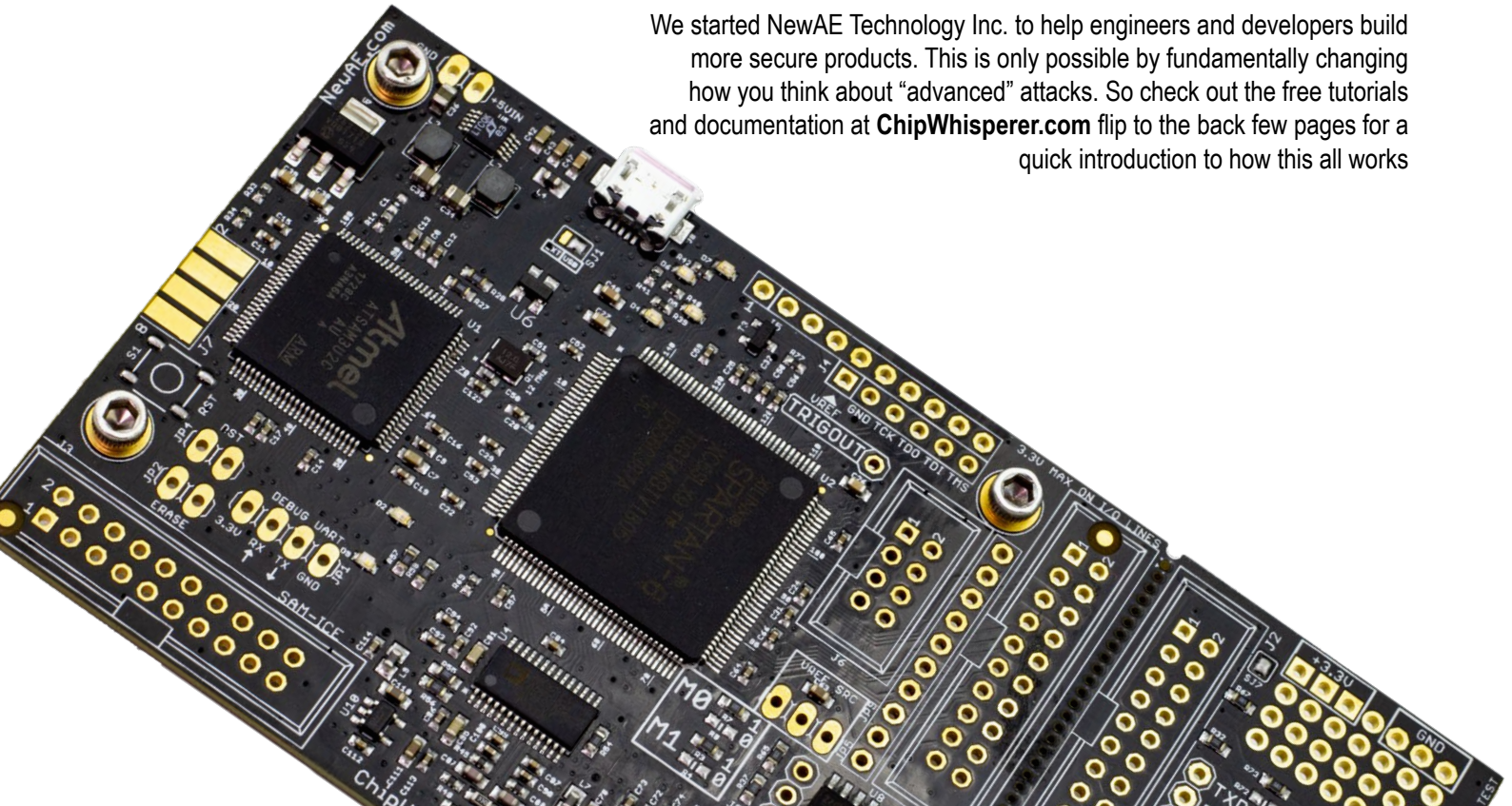
HELLO NERDS,

Welcome to a world where you can recover AES-256 keys in minutes from most software libraries, and many hardware accelerators. A world where you can't trust software alone, and hardware is looking pretty shady too.

It's the world your products live in, whether you want to believe it or not. So why not find out how to test them yourself, so you can beat the FUD and decide on real security solutions that solve real problems.

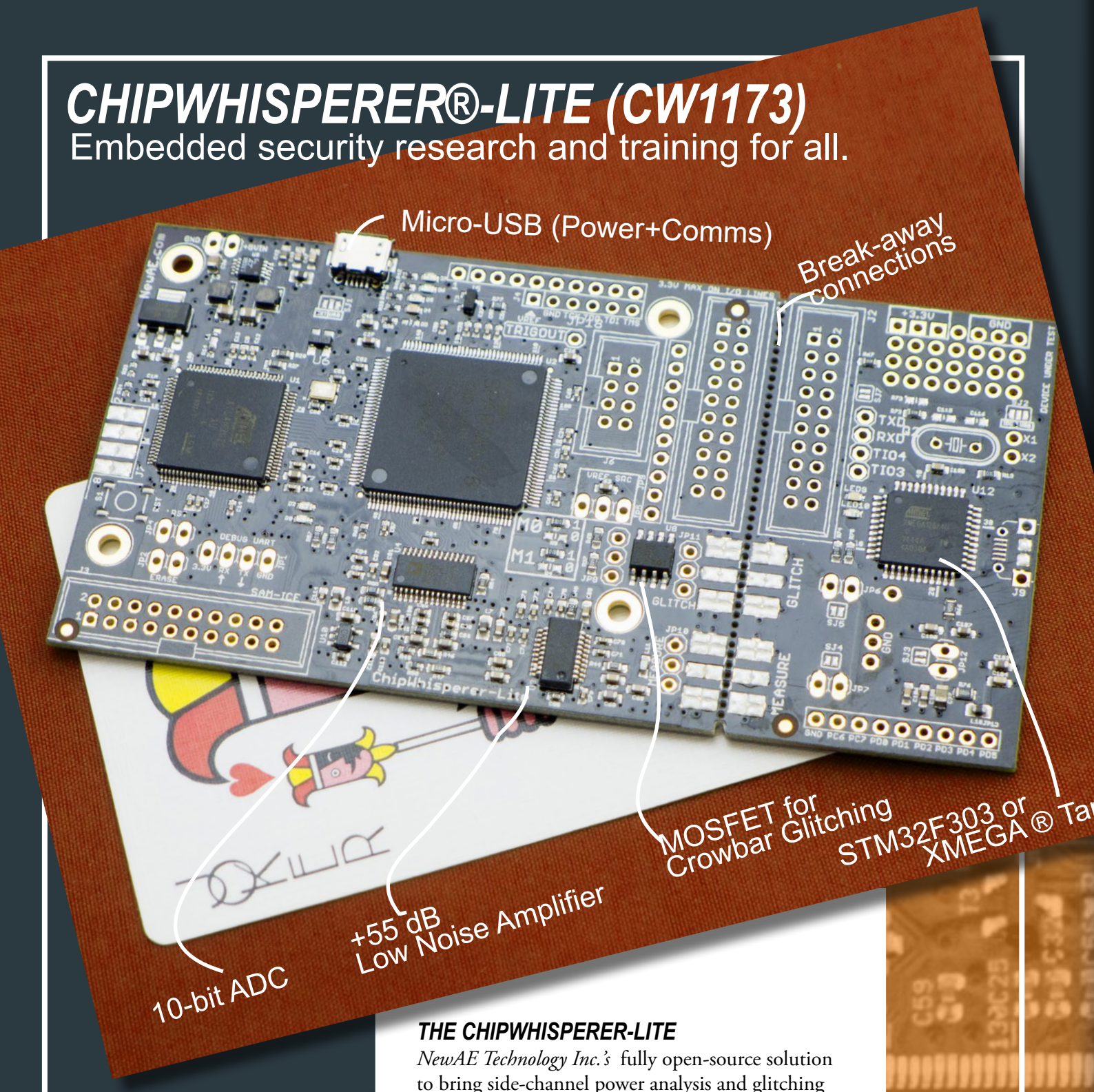
OPEN-SOURCE. FOR REAL.

We started NewAE Technology Inc. to help engineers and developers build more secure products. This is only possible by fundamentally changing how you think about "advanced" attacks. So check out the free tutorials and documentation at **ChipWhisperer.com** flip to the back few pages for a quick introduction to how this all works



CHIPWHISPERER®-LITE (CW1173)

Embedded security research and training for all.



THE CHIPWHISPERER-LITE

NewAE Technology Inc.'s fully open-source solution to bring side-channel power analysis and glitching attacks to every enegineer and student. Completely open-source design (hardware, software, firmware), as a result of a successful Kickstarter in Spring 2015.

The ChipWhisperer-Lite integrates hardware for performing power analysis measurement, device programming, glitching, serial communications, and an example target that can be loaded with cryptographic algorithms all into a single board. Now available in a 32-bit edition (with STM32F303 target) or XMEGA target to perform analysis on a wide variety of cryptographic libraries and security solutions.

SPECIFICATIONS & ORDERING

Feature	Notes/Range
ADC Specifications	10-bit ADC, 105 MS/s maximum sample rate.
ADC Sample Clock Source	Internal generator, external input (direct or with 4x multiplier or phase adjuster).
Analog Input	AC-Coupled, up to +55dB adjustable gain.
GPIO Types	Serial, clock, logic line (i.e., for reset pin).
GPIO Voltage	3.3V.
Clock Generation Range	5-200 MHz.
Clock Output Type	Regular, with glitch inserted, only output glitch.
Glitch Width (min)	~1nS (depends on cabling used for routing glitch output).
Glitch Offset	Adjustable in < 200pS increments.
Voltage glitch type	High-power and low-power crowbar circuitry.
Crowbar pulse current	20A.
USB Interface	Custom open-source USB firmware, up to 25 MB/s speed.
Sample Buffer Size	24 573.
Target Device	Atmel XMEGA128D4 (on classic device).
Programming Protocols	Atmel ISP (for AVR), Atmel PDI (for XMEGA), STM32Fx Bootloader

NAE-CWLITE ..... Single-board solution, XMEGA Target.
NAE-CWLITE-ARM ..... Single-board solution 32-bit edition, STM32F3 Target.
NAE-CWLITE-CAPTURE ..... Capture board only, requires external target (such as UFO Board).

2-PART VERSION OR REGULAR?

The single-board version (NAE-CWLITE-04) is perfect when you don't expect to connect to external targets, or want the most compact solution.

The -CAPTURE version gives you the flexibility to connect up additional targets, and is included in our Level 1 & Level 2 starter kits.

It's always possible to "break" the single-board version into the 2-Part version if you change your mind.

STARTER KITS
expand your horizon

SIDE-CHANNEL ANALYSIS

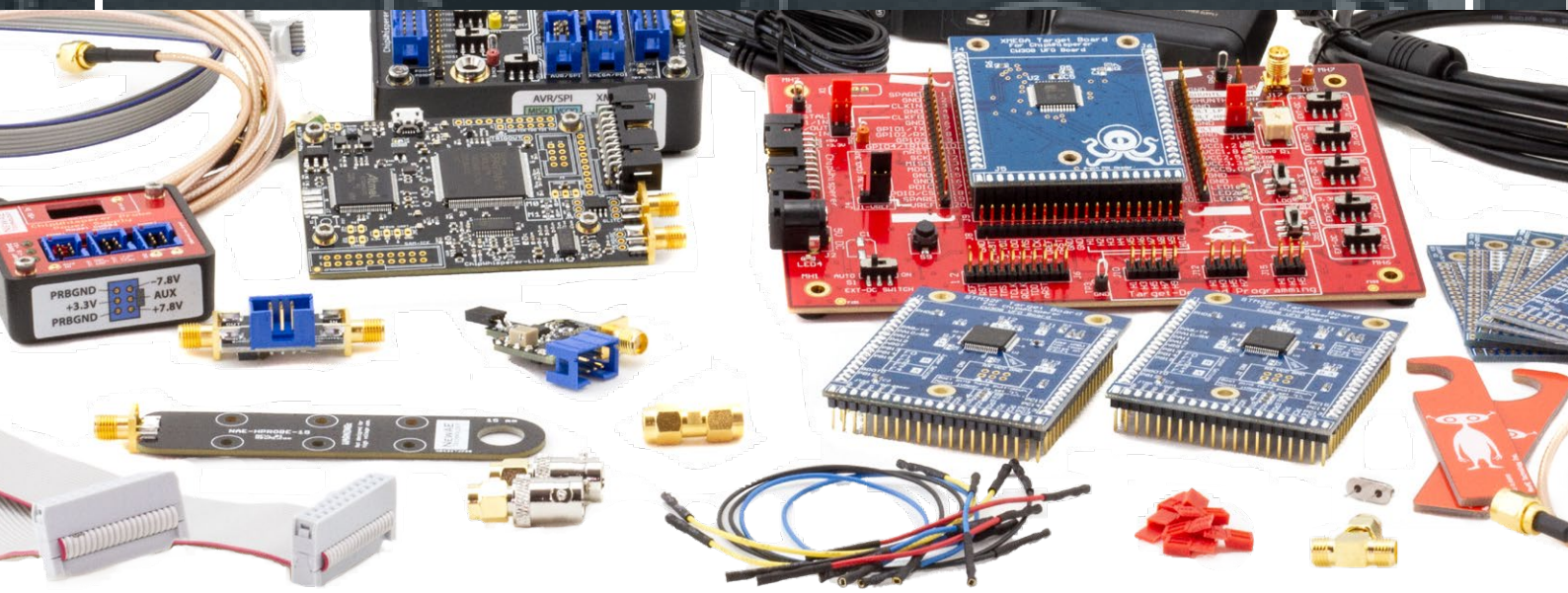
105 MS/s 10-bit ADC with +55 dB Low Noise Amplifier allows the measurement of small, high-frequency signals characteristic of power analysis measurements.

Advanced clock routing fabric allows generation of arbitrary frequencies, or use of external clocks for sampling.

GLITCHING ATTACKS

FPGA-based glitch generator XORs two phase-shifted clocks together to generate an arbitrary number of glitches, perfectly synchronized to device clock.

Glitches can be inserted into the clock, used to trigger built-in crowbar, or routed to external glitch circuitry.



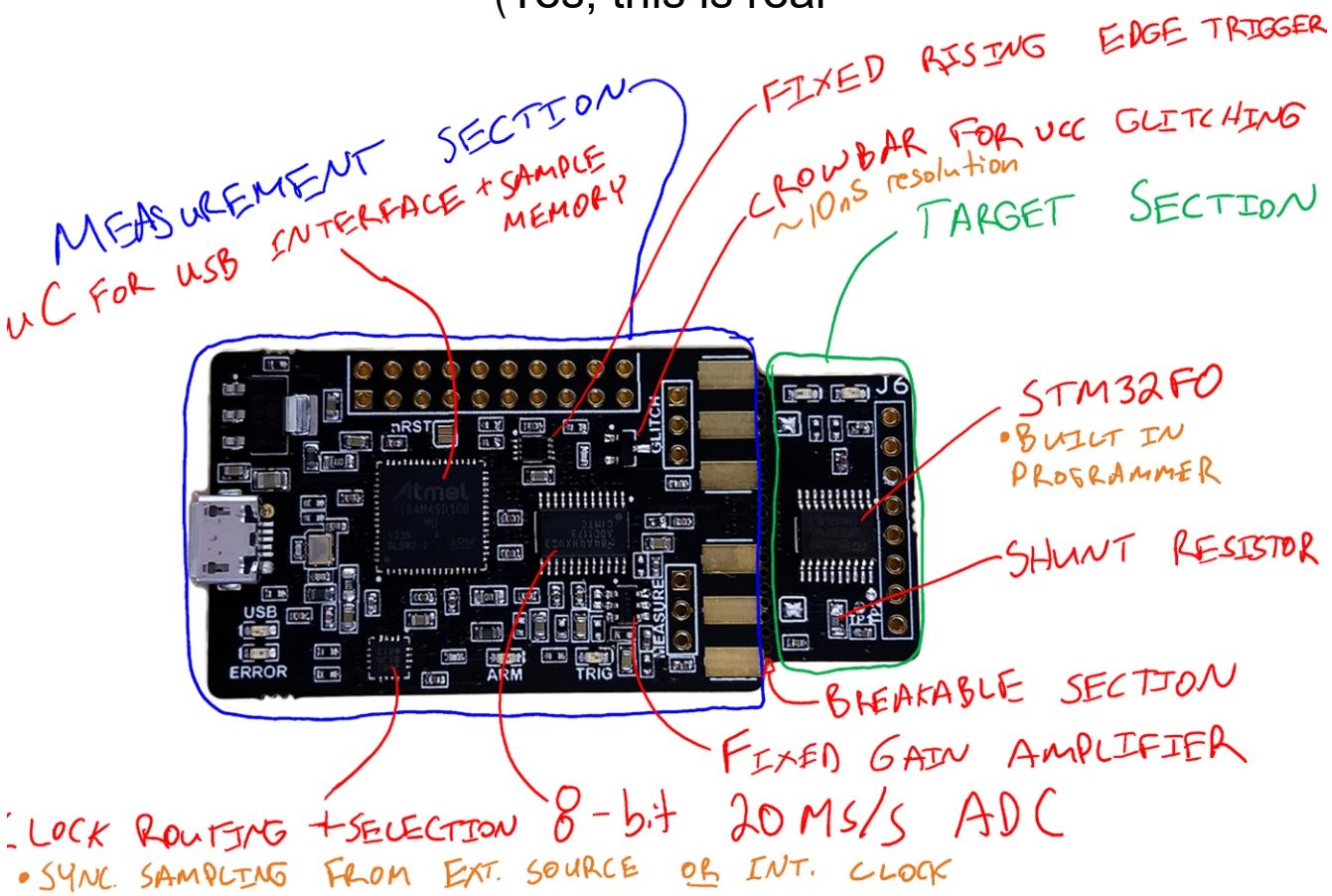
All products subject to extensive QA checks by our QA manager Luna.

Introducing the assistant to the QA manager to help with the expanding product lines, Bergen

HOW LOW CAN YOU GO?

POWER ANALYSIS FOR $50

(Yes, this is real



CHIPWHISPERER®-NANO (CW1101)

THE CHIP WHISPERER - NANO

Represents NewAE Technology Inc most agressive pursuit of its mission to bring side-channel power analysis to everyone. Build out a training program to teach your customers about side-channel power analysis and how your solutions help. Ask about our ability to offer customized solutions or a module-based design so you can ChipWhisper enable your development board.

The ChipWhisperer-Nano integrates hardware for performing power analysis measurement, device programming, serial communications, and an example target that can be loaded with cryptographic algorithms all into a single board.

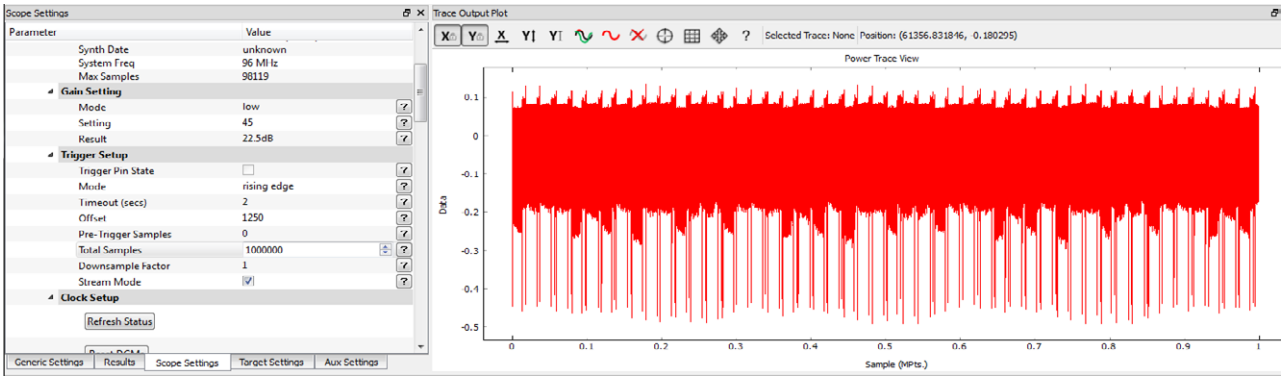
CW1200 CHIPWHISPERER-PRO

STREAM MODE FOR LONGER CAPTURES

If you are running less than 10MS/s, you can stream data back over USB. Combine that with the new hardware downsampling mode so you can keep the ADC perfectly synchronized with your faster target device. It simplifies exploration of asymmetric and other very long algorithms.

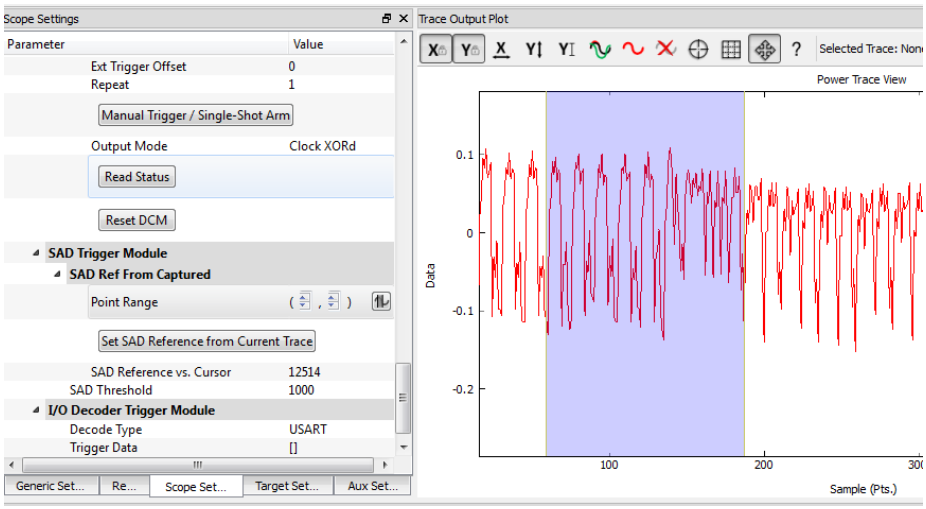
The ChipWhisperer-Pro has been designed to remain compatible with existing Chip-Whisperer-Lite interfaces, but adds new features, thanks to a larger internet FPGA.

It also comes with handy accessories, such as a 500 kHz high-pass and a 20 Mhz low-pass filter. It is available in a convenient starter pack with a waterproof case (maybe you want to take this on your next hiking trip?).



SAD TRIGGER MATCH

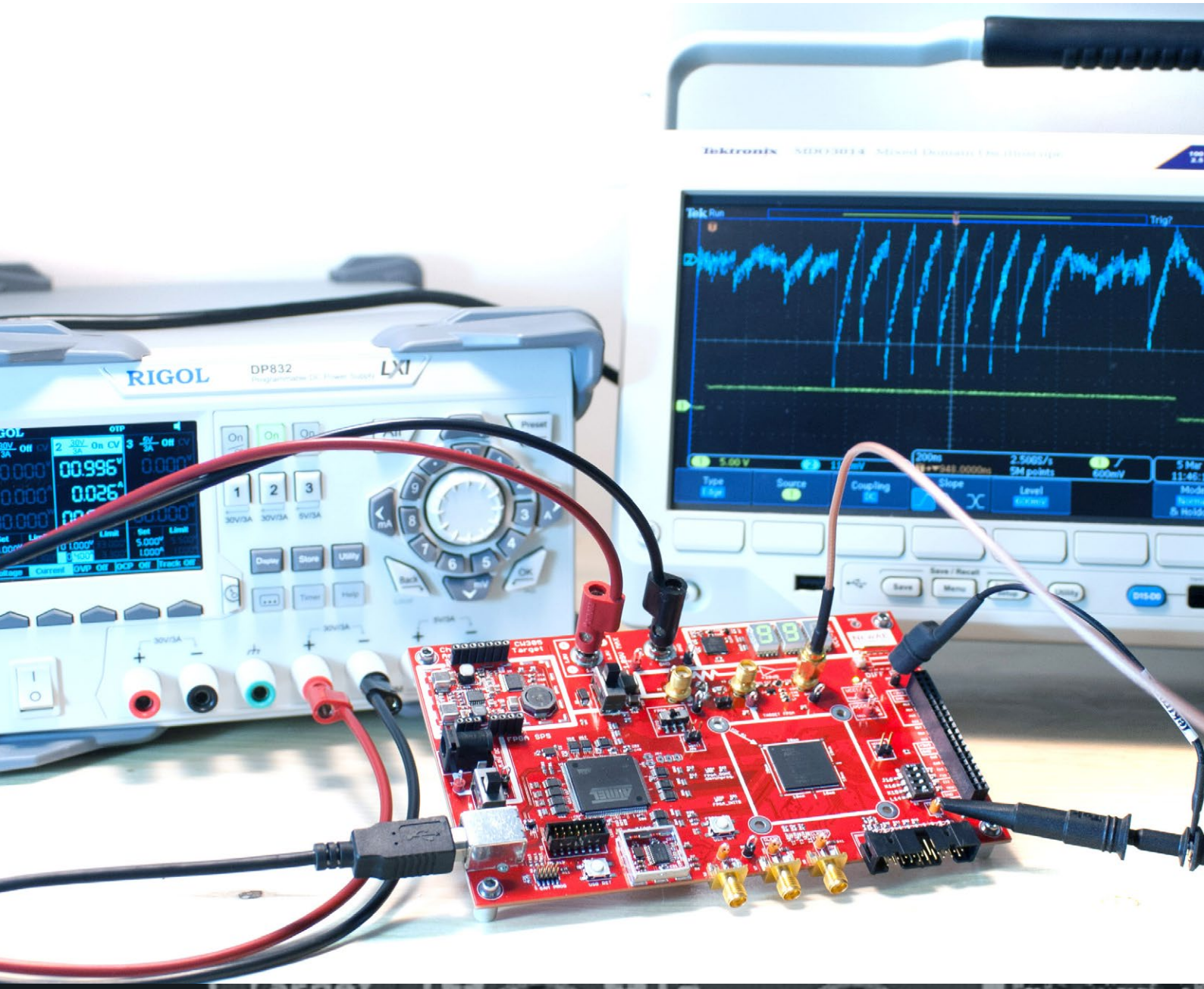
Easily take a portion of your capture to waveform and use that to trigger both capture and glitch systems. Perfect for synchronizing in hardware.



SPECIFICATIONS & ORDERING

Feature	Notes/Range
ADC Specifications	10-bit ADC, 105 MS/s maximum sample rate.
ADC Sample Clock Source	Internal generator, external input (direct or with 4x multiplier or phase adjuster).
Analog Input	AC-Coupled, up to +55dB adjustable gain.
Trigger Sources (Glitch & ADC)	Edge, Level, SPI data, UART data, analog pattern (SAD Trigger).
SAD Trigger	128-point pattern, real-time matching (approx. 4-cycle delay*).
AUX Functions	Trigger In, Trigger Out.
GPIO Types	Serial, clock, logic line (i.e., for reset pin).
GPIO Voltage	3.3V.
Clock Generation Range	5-200 MHz.
Clock Output Type	Regular, with glitch inserted, only output glitch.
Glitch Width (min)	~1nS (depends on cabling used for routing glitch output).
Glitch Offset	Adjustable in < 200pS increments.
Voltage glitch type	High-power and low-power crowbar circuitry.
Crowbar pulse current	20A.
USB Interface	Custom open-source USB firmware, up to 25 MB/s speed.
Streaming Speed	Unlimited buffer size (limited by computer) up to 10 MS/s.
Sample Buffer Size	98119.
Programming Protocols	Atmel ISP (for AVR), Atmel PDI (for XMEGA), STM32Fx Bootloader

* SAD match processing takes 4 ADC cycles after 128-sample match comparison. ADC and capture circuitry has approximately 8 ADC cycle delay between analog front-end and data available internally.



CW305 ARTIX® FPGA TARGET

SCA, GLITCH ATTACKS, PUF DESIGN

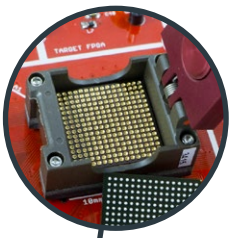
The CW305 has been designed from the ground-up to give you the best platform for embedded security research on FPGAs. A custom USB interface chip means you can trivially send and receive data to your FPGA design, while also performing FPGA configuration and adjusting external PLL operating frequencies all from the same interface. ESD Protection on all I/O lines allows you to perform glitch insertion safely, and an optional BGA socket is perfect for comparing effects across many physical devices.

Starting at $800 USD

CW305: THE FPGA PLAYGROUND

LOADED WITH FEATURES FOR ALL YOUR FPGA EXPERIMENTS.

Optional socket available!



Banana jacks simplify connection to bench supply for VCC-INT.

Adjustable VCC-INT regulator (controlled via USB) lets you check PUF operation at different voltages.

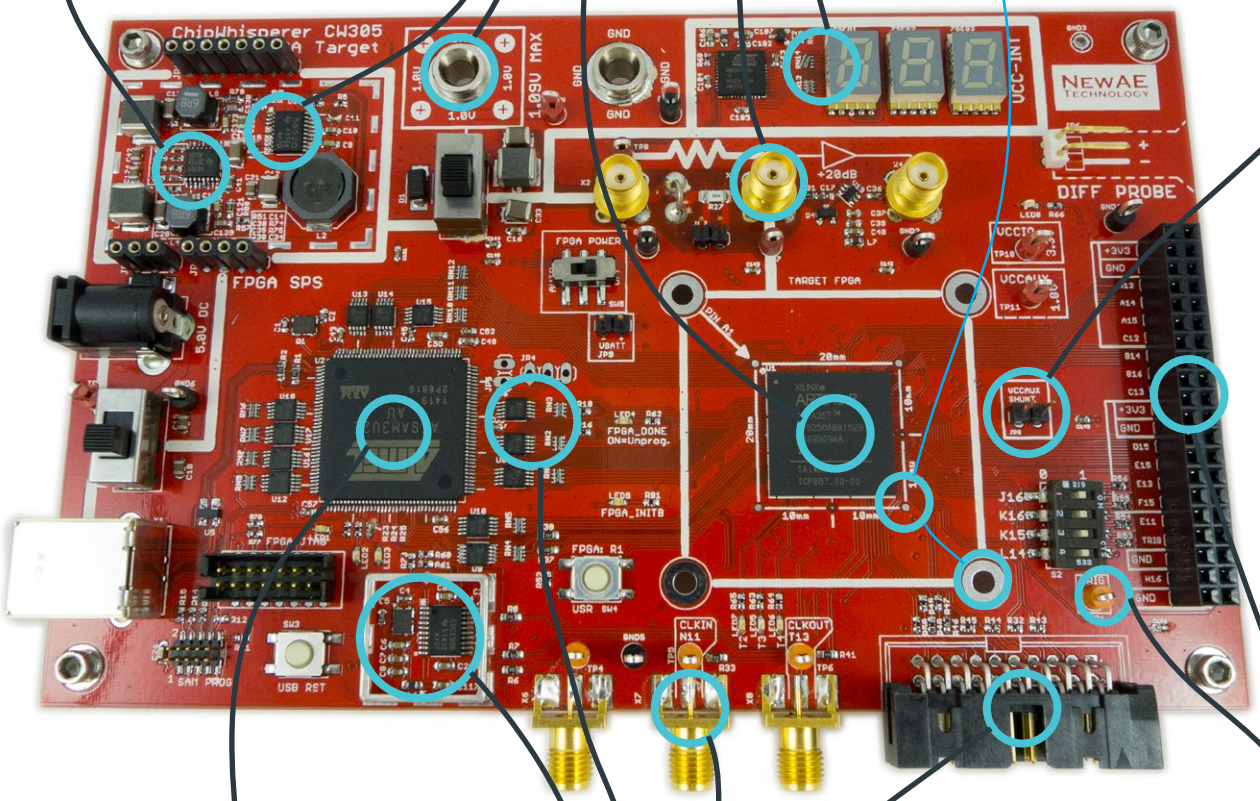
VCCIO/VCCAUX regulator with optional low-noise linear add-on.

SMA connectors for power measurement & voltage fault insertion. +20dB amplified output simplifies connection to scope.

DMM to monitor FPGA core voltage.

VCC-AUX shunt for additional measurement experiments.

PCB targets and mounting holes for X-Y table alignment.



Custom USB interface provides API to directly read/write into FPGA memory space, along with FPGA configuration in 2 seconds.

External PLL generates from 1 MHz - 200 MHz clock frequency for FPGA, perfect for validating SCA or PUF operation at different frequencies, without having to modify the FPGA.

Diode protection to prevent target voltage glitches from affecting USB interface chip.

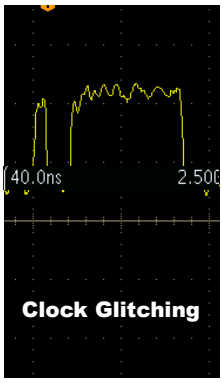
Numerous test points for use with regular scope.

Expansion header for additional I/O.

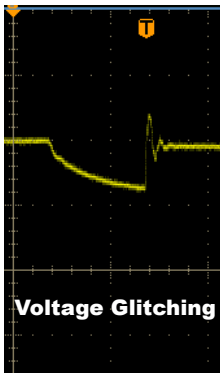
20-Pin Connector for ChipWhisperer capture hardware.

SMA connectors for clock input/output.

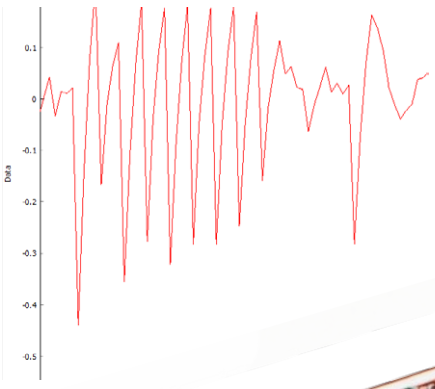
TOOLCHAIN USAGE



Easily generate clocks with a wide variety of glitches using the ChipWhisperer's FPGA-based glitch generator logic.



Crowbar glitching generates precisely timed glitches that exploit the power distribution network (PDN) to cause a wide array of effects in the target device.



Easily and reliably measure power signatures using the ChipWhisperer capture's synchronous sampling architecture.

CW305 + CHIPWHISPERER CAPTURE

SIDE-CHANNEL ANALYSIS

SMA connector provides low-noise measurement output to the ChipWhisperer.
A header for use of optional differential probe (requires probe + probe power supply).

GLITCHING ATTACKS

ChipWhisperer-Capture can generate glitchy clocks to feed into CW305.
SMA connectors allow insertion of voltage glitches using crowbar.

Specifications & Ordering

Feature	Notes/Range
FPGA Supported	Artix-7 in FTG256 Package.
FPGA Configuration support	USB (built in), JTAG (requires external tool), SPI Flash memory.
Power Supplies	0.8-1.2V (VCC-INT), 4A, Programmable. 1.8V (VCC-AUX), 1.5A, Fixed. 3.3V (VCC-IO), 2A, Fixed.
USB Interface	Custom high-speed USB 2.0 firmware running on ARM microcontroller.
USB Functions	FPGA configuration, VCC-INT setting, PLL configuration, writing onto data-bus for FPGA.
USB Example Languages	Python (Linux, Windows, Mac OS-X).
USB Supported Language	Any that can access libusb DLL (C, C++, VB, etc).
Supported Toolchains	Xilinx Vivado (All FPGAs), Xilinx ISE (XC7A100T only).
PLL Channels	3 separate frequencies.
PLL Output Range	1-200 MHz.
I/O on Expansion Header	27 GPIO (including 2x differential & 3 clock inputs on FPGA).
I/O on 20-pin Header	11 GPIO (including 1 clock input on FPGA).
I/O on SMA Connectors	2 GPIO (including 1 clock inputs on FPGA).

As the CW305 contains many options, you can build a part number to specify different options, such as mounting the BGA socket (shown at right).

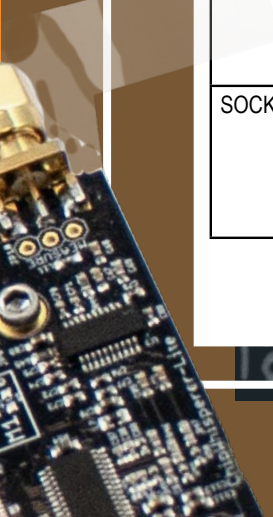
Revision (04)

NAE-CW305-04-7A35-0.25-X

Shunt value (ohms) - see https://store.newae.com

CODE	FPGA	NOTES
7A35	XC7A35T-2FTG256	Suitable for most symmetric cryptographic implementations (i.e., pipelined AES will fit). Must use Vivado toolchain (ISE only supports the XC7A100T).
7A100	XC7A100T-2FTG256	Large FPGA with 3x logic resources of 7A35. Suitable for very large crypto implementations. Can use either ISE or Vivado.
SOCKET	BGA socket with heatsink.	No FPGA provided in socket, supports any Artix-7 in FTG256 package. Perfect for comparison between devices, such as for PUFs or template attacks.

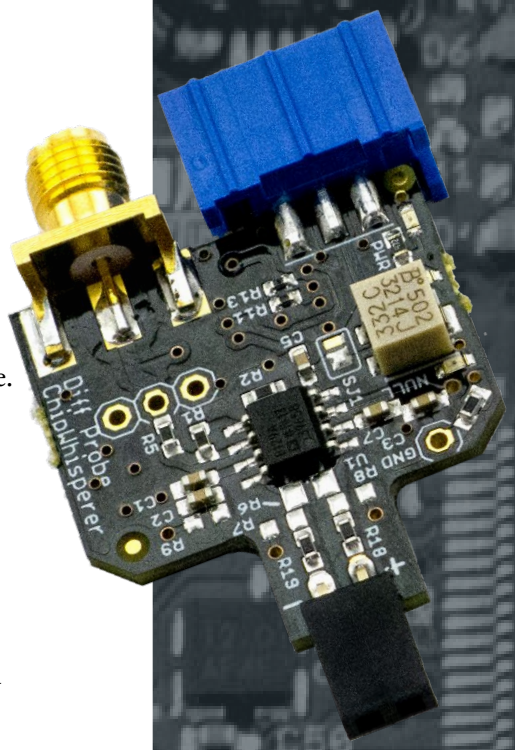
CODE	PDN	NOTES
X	No VCC-INT Capacitors	The decoupling capacitors on the VCC-INT network are NOT present. This option is required if performing side-channel power analysis using the current shunt.
M	VCC-INT Capacitors	The decoupling capacitors on the VCC-INT network are present. Generally if using the board primarily for PUF analysis or fault injection, this option is suitable.

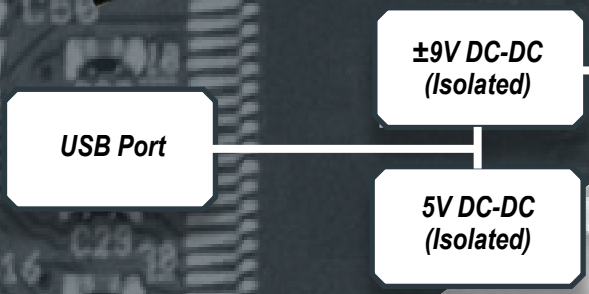


DIFFERENTIAL PROBE

LOW COST DIFFERENTIAL PROBE

- Usable over 20 kHz - 200 MHz.
- Can be used down to DC with jumper change.
- 10x gain.
- Adjustable DC-offset null.
- LED feedback for null voltage setting.
- Based on AD8129 Differential
- Amplifier.
- Usable on both VCC and GND shunts.
- Can operate on VCC shunt with single-ended power supply, requires dual-ended supply for GND shunts.





PLANAR H-FIELD PROBE + LNA

PCB-BASED H-FIELD PROBE

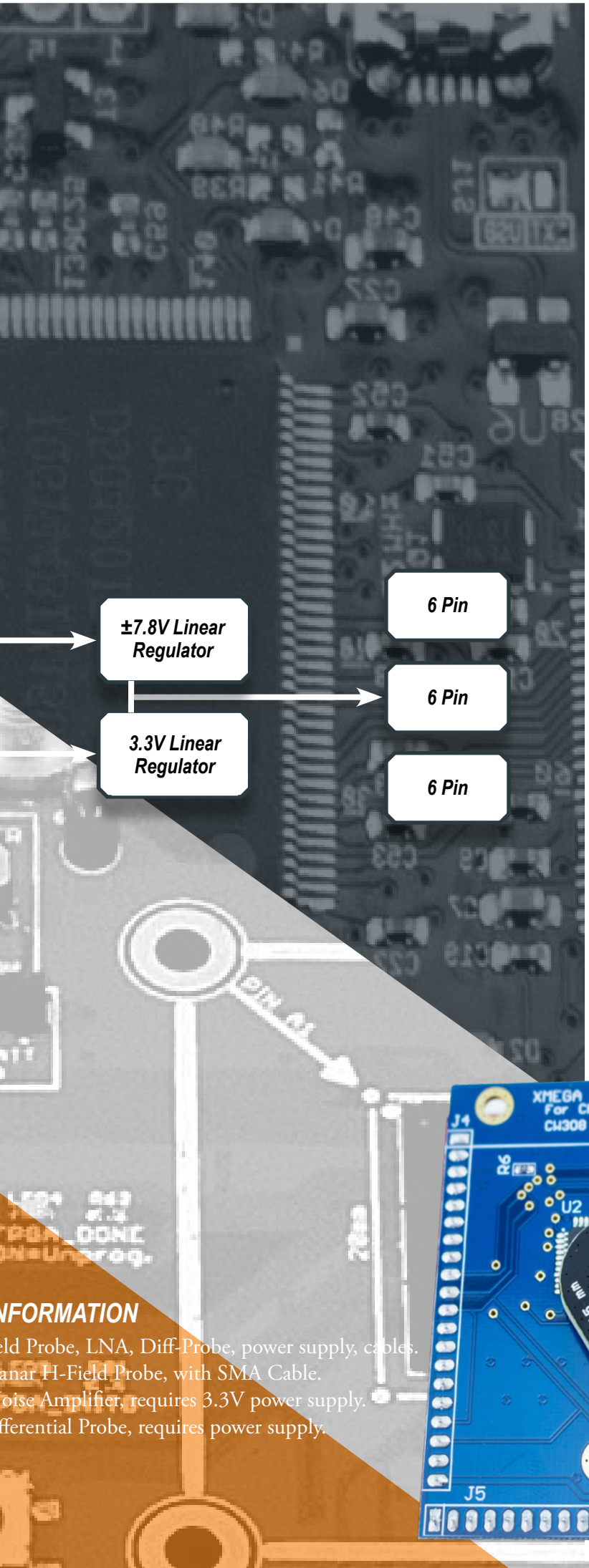
- Requires 3.3V Power.
- Mounts onto H-Field probe to minimize potential for noise coupling.

+20DB LOW NOISE AMPLIFIER

- 15 mm loop diameter.
- 6x mounting holes.
- Standard SMA connector for integration with existing equipment.
- Can be used for measurement or EM insertion.

ORDERING IN

NAE-PBSET-PSU-03 ..... Set with H-Fie
NAE-HPROBE-15 ..... Pl
NAE-LNA-02 ..... Low N
NAE-DIFFPROBE-02 ..... Di



SIMPLE PROBE-SET

- Micro-USB for 5V power input.
- Input power isolated to avoid ground loops with power source and target.
- Power-good LEDs provide indication of working power supply unit (PSU).
- Power Supply provides ±7.8V for differential probe and +3.3V for Low Noise Amplifier.

MAGNETIC FIELD PROBING

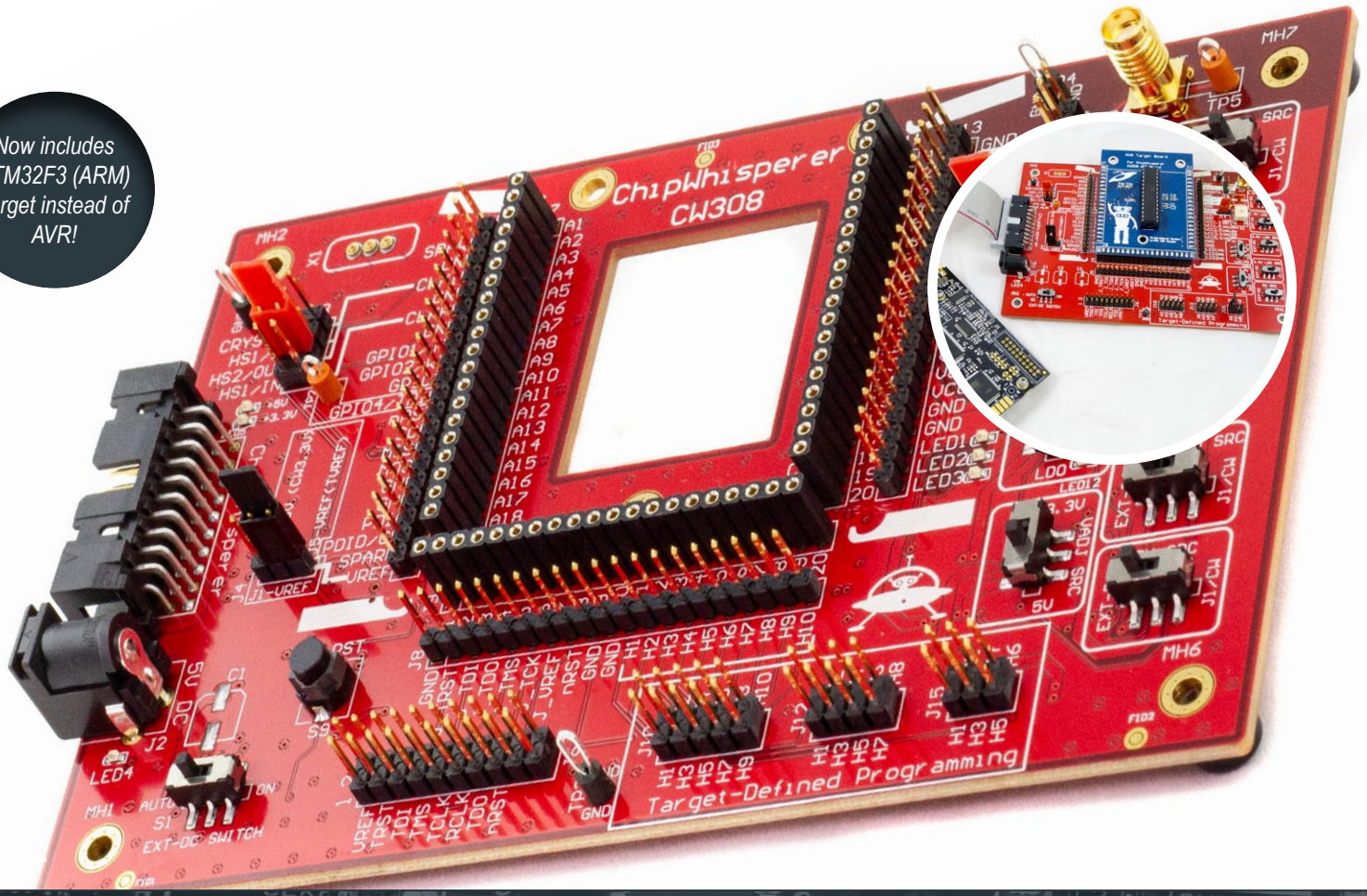
- Changing current draw through target device causes a changing magnetic field.
- H-Probe picks up magnetic field, and creates voltage proportional to field.
- ChipWhisperer digitizes this waveform, and recovers the side-channel information required for a successful attack.

NFORMATION

eld Probe, LNA, Diff-Probe, power supply, cables.
anar H-Field Probe, with SMA Cable.
oise Amplifier, requires 3.3V power supply.
fferential Probe, requires power supply.

UFO TARGET BOARD(CW308)

Now includes STM32F3 (ARM) Target instead of AVR!



TARGET CONNECTIONS

Provides power, clock, and filtering for DPA attacks.

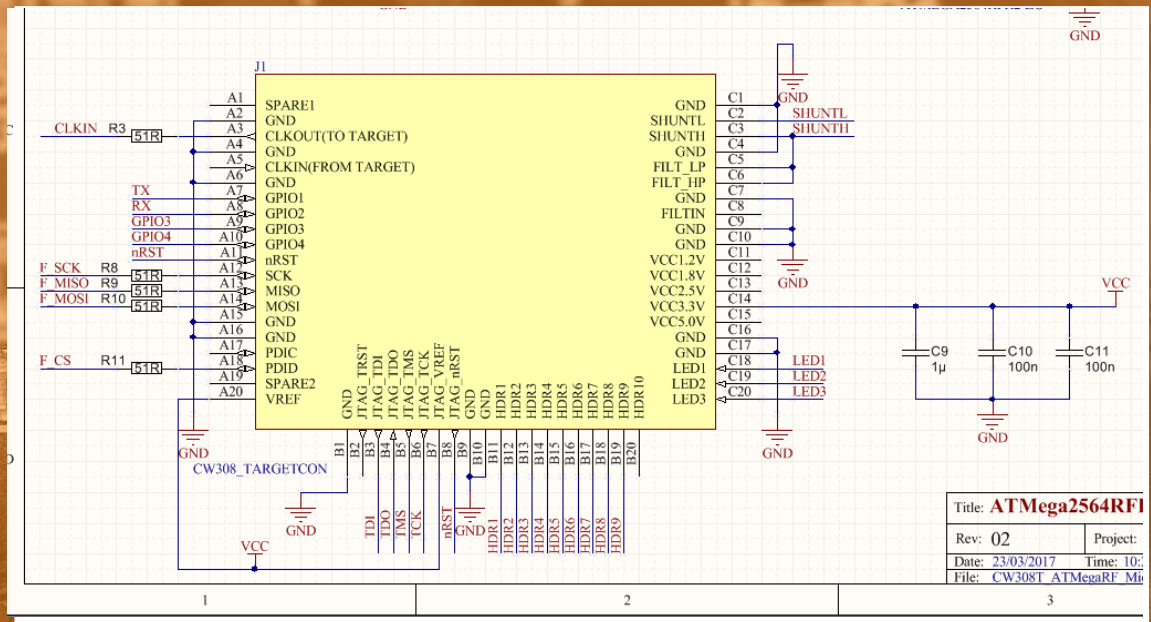
Supports multiple chip families, and easy to extend for new chips.

Prototype-board allows use of new chips without spinning PCB.

Use stand-alone with your own oscilloscope.

Use standard 20-pin connector for integration with our various capture solutions..

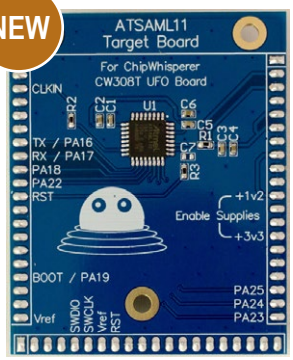
SIMPLIFIED TARGETS



The CW308 provides a simple support board, letting you quickly validate and test new devices. Save time respinning custom target boards, and easily share them with the wider community.

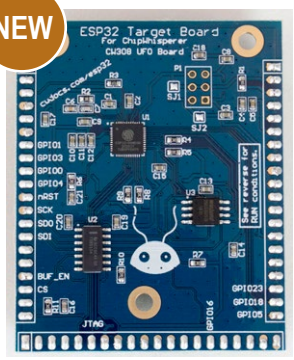
SAML11
Cortex M23

NEW



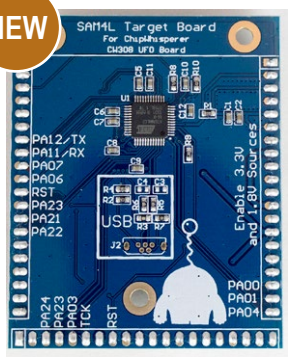
ESP32
Secure Boot

NEW

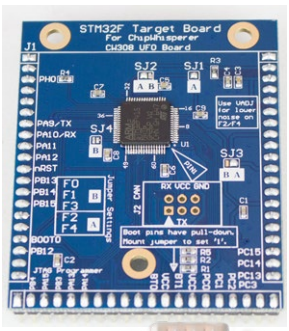


SAM4L
DPA 'Countermeasures'

NEW



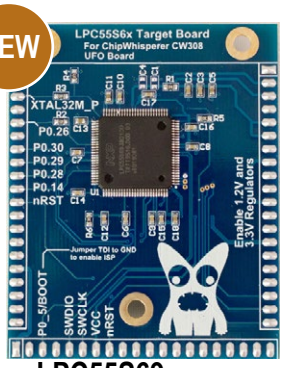
STM32F0/1/2/3/4
Cortex-M0/M1/M3/M4



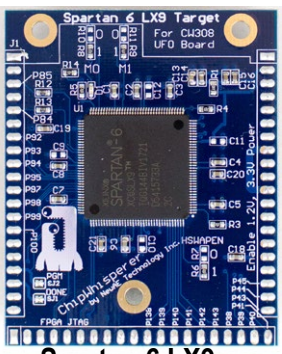
NEW

K82F
Masked AES, Trace Port

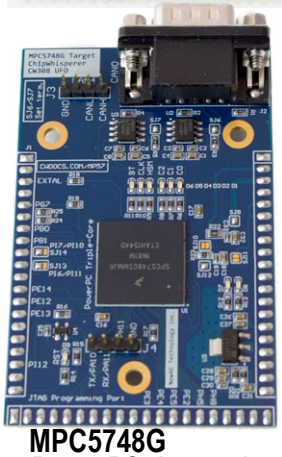
NEW



LPC55S69
Cortex M33, PUF



Spartan 6 LX9
Small FPGA

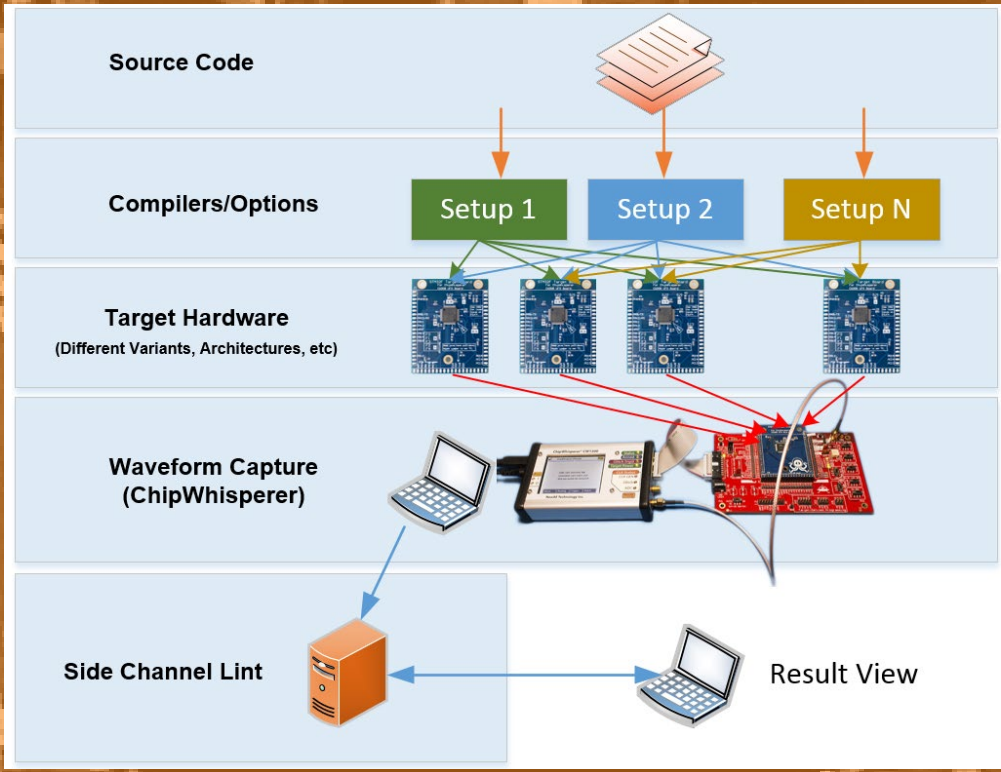


MPC5748G
Power-PC, Automotive

WITH CHIPWHISPERER-LINT

LIBRARY VALIDATION

Validate your IP (libraries or hardware core) against power analysis leakage. Find problems before your customer does.



Source code is crypto library under test (for SW), but can be IP core for FPGA tests.

Various binaries generated – library is compiled for supported platforms and with various options a user might enable.

Binaries loaded onto test platform (for example, based on UFO board), but can also use existing development kits that have been instrumented to take power measurements.

Capture can be done with regular oscilloscope. Here ChipWhisperer hardware (open-source versions available) shown, which simplifies setup considerably.

Captured power traces analyzed by ChipWhisperer-Lint. Can run a local server or use more powerful cloud style server.

Side-Channel Lint Test Report

Report generated at 2017-07-07 16:29:04.026000

Test Results

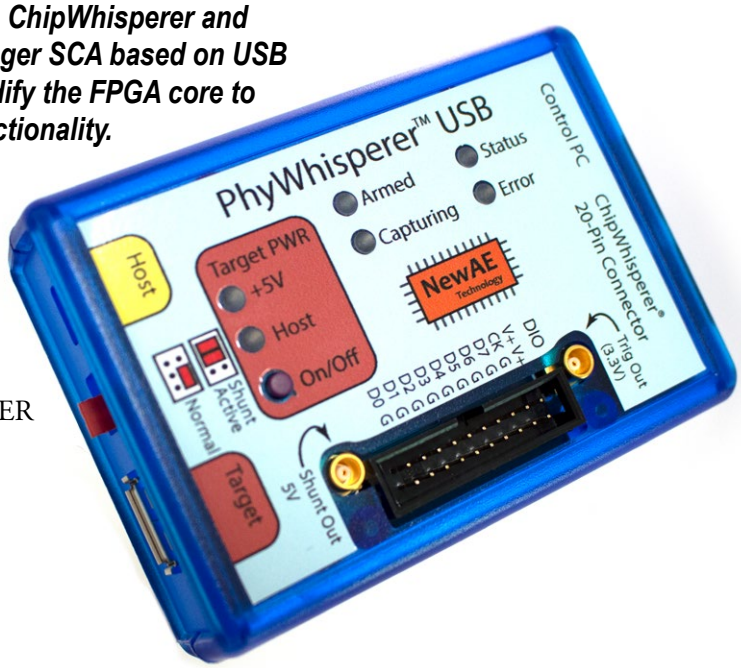
1. ROM vs. RAM Tables
2. Optimization Off vs. On
3. IAR vs GCC Compiler
4. STM32F0 vs STM32F1 vs STM32F2

Test Number	Test Name	STM32F0: GCC, OPT=0, RAM Tables	STM32F0: GCC, OPT=0, ROM Tables	STM32F0: GCC, OPT=s, RAM Tables	STM32F0: GCC, OPT=s, ROM Tables	STM32F0: IAR, OPT=0, RAM Tables	STM32F0: IAR, OPT=0, ROM Tables	STM32F0: IAR, OPT=s, RAM Tables	STM32F0: IAR, OPT=s, ROM Tables	STM32F1: GCC, OPT=0, RAM Tables	STM32F1: GCC, OPT=0, ROM Tables	STM32F1: GCC, OPT=s, RAM Tables	STM32F1: GCC, OPT=s, ROM Tables	STM32F1: IAR, OPT=0, RAM Tables	STM32F1: IAR, OPT=0, ROM Tables	STM32F1: IAR, OPT=s, RAM Tables	STM32F1: IAR, OPT=s, ROM Tables	STM32F2: GCC, OPT=0, RAM Tables	STM32F2: GCC, OPT=0, ROM Tables	STM32F2: GCC, OPT=s, RAM Tables	STM32F2: GCC, OPT=s, ROM Tables	STM32F2: IAR, OPT=0, RAM Tables	STM32F2: IAR, OPT=0, ROM Tables	STM32F2: IAR, OPT=s, RAM Tables	STM32F2: IAR, OPT=s, ROM Tables
-	Minimum Time	10147	10147	7147	7143	9963	9963	6699	6691	8795	4475	7055	4071	11659	17259	7283	10747	9967	6363	9559	
-	Maximum Time	10147	10147	7147	7143	9963	9963	6699	6691	8795	4475	7055	4071	11659	17259	7283	10847	9967	6363	9655	
1	HW: Plaintext	20.058	23.162	46.461	48.719	15.408	14.293	15.215	17.111	19.737	6.457	14.728	10.381	14.733	15.471	2.675	7.373	3.710	2.918	5.449	
2	HD: Plaintext to Key	15.928	16.230	14.478	13.311	18.310	18.810	18.035	18.881	16.802	19.151	15.109	13.497	9.993	14.722	2.500	5.302	4.647	5.076	3.483	
3	HD: Plaintext to Round 0: AddRoundKey Output	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
4	HD: Plaintext to Round 1: SubBytes Output	2.681	2.623	4.164	2.105	2.363	2.606	2.056	2.538	2.258	2.094	2.667	2.584	2.589	2.605	2.734	2.243	2.532	2.098	3.767	
5	HD: Plaintext to Round 1: ShiftRows Output	2.681	2.623	4.164	2.105	2.363	2.606	2.056	2.538	2.258	2.094	2.667	2.584	2.589	2.605	2.734	2.243	2.532	2.098	3.767	
6	HW: Key	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	
7	HD: Key to Round 0: AddRoundKey Output	20.058	23.162	46.461	48.719	15.408	14.293	15.215	17.111	19.737	6.457	14.728	10.381	14.733	15.471	2.675	7.373	3.710	2.918	5.449	

PHYWHISPERER-USB

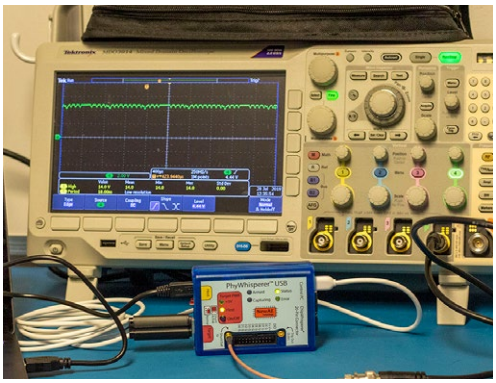
OPEN SOURCE USB TRIGGERING & SNIFFING

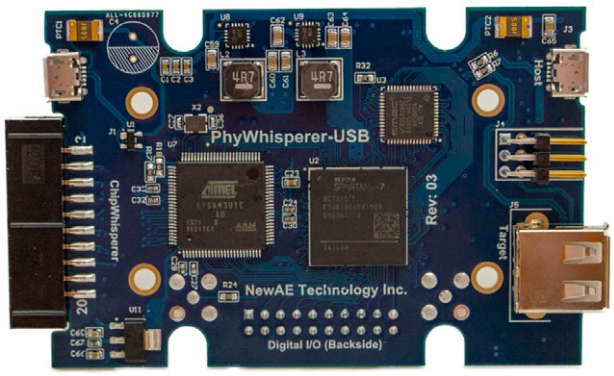
Sniff and trigger on USB data packets. Connects to ChipWhisperer and ChipSHOUTER tools to allow injecting faults or trigger SCA based on USB traffic. Fully open-source design allows you to modify the FPGA core to add your own logic, or to build more advanced functionality.



- USB 2.0 LS/FS/HS support.
- Trigger on USB data sequence.
- Sniff USB traffic, including detecting errors.
- Toggle target power from API or front panel button.
- Logic-level trigger output, connect to ChipSHOUTER or other lab gear.
- USB clock can be routed to ChipWhisperer for synchronous sampling.
- In-line shunt resistor for simple power analysis.
- Open-source design, including Spartan 7 FPGA.

GITHUB.COM/NEWAETECH/PHYWHISPERERUSB





CHIPSHOUTER ®

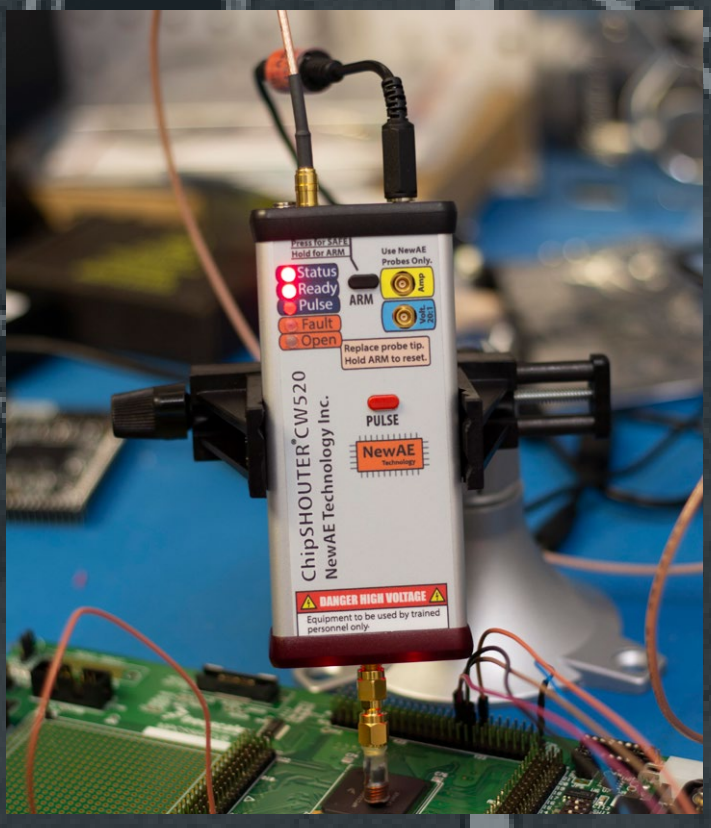
Electromagnetic Fault Injection

See https://www.github.com/newaetech/ChipSHOUTER for full user manual, API documentation, and more!

Our first electromagnetic fault injection tool uses low-ESR capacitors to dump up to 500V through various E.M. probes. Digital control of charge voltage, and fast response times provides you with the E.M. fault inection tool that simplifies your fault investigations. Multiple calibration targets, and upcoming XY table provide a complete solution for your needs.

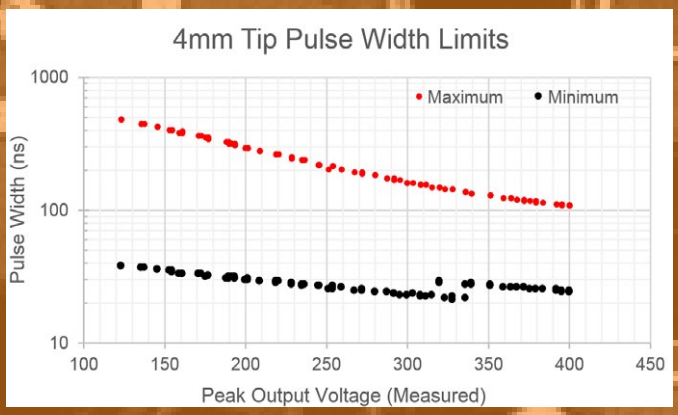
KIT CONTENTS:

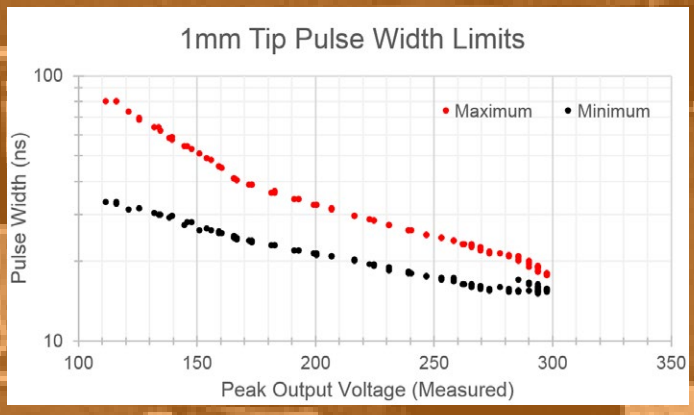
- ChipSHOUTER CW520 Box
- Ballistic Gel EMFI Target (CW521)
- Simple EMFI Target (CW322)
- Oscilloscope adapters (x2)
- EMFI Injection Tips (x4)
- SMB Cable
- SMB to BNC Cable (for trigger input)
- SMB to SMA Cable (for trigger input)
- Isolated USB Interface
- 19V/3.4A Power Adapter
- USB and Data Cables



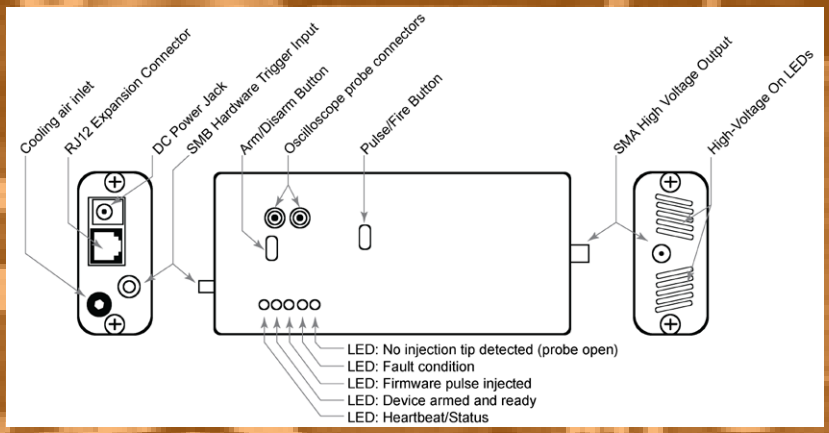
Feature	Notes/Range
Trigger Modes	(1) Basic (2) Programmable waveform (3) External hardware trigger
Hardware Trigger	SMB Conenctor, 1.8KΩ or 50Ω, active high or low
Waveform monitor output	BNC connector for use with 1MΩ || 10-25pF oscilloscope input, 20:1 attenuation on voltage monitor
Voltage range (set)	150V to 500V
Change voltage rate	30-40 V/ms
Trigger (Basic) Pulse Length	80-960nS, in 80nS steps
Trigger (Programmable) Steps	20.83 nS time step, 1-5000 time steps in each pulse
Hardware Input delay	75nS (typ)
Hardware Input jitter	150 pS std-dev (typ)
1mm injection tip pulse width	15 - 80nS (typ)
4mm injection tip pulse width	24 - 480nS (type)
Injected pulse width jutter	350 pS std-dev (typ)
Pulse spacing, 4mm tip, 500V charge voltage	2 pulses: 100nS (typ) 3 pulses: 175nS (typ)
Interface protocols	(1) Interactive serial command prompt (2) Binary serial protocol with Python 3 API

The following shows typical results of the minimum injection pulse width for various voltages with the two provided tip geometries. The tip characteristics limit the pulse width the ChipSHOUTER can achieve:





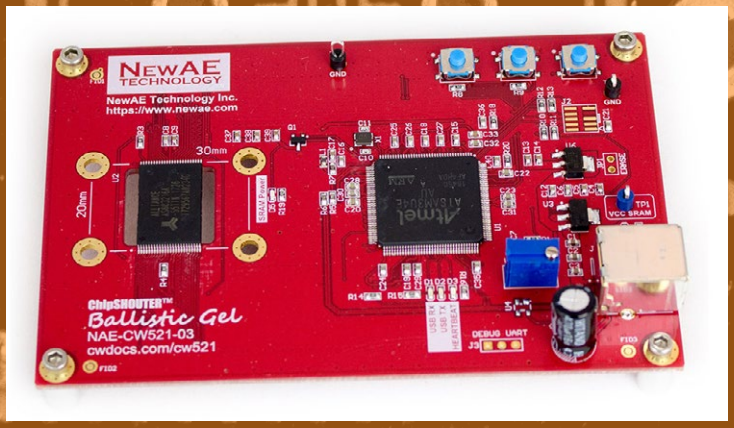
The following shows ChipSHOUTER external connections:



CHIPSHOUTER® TARGETS

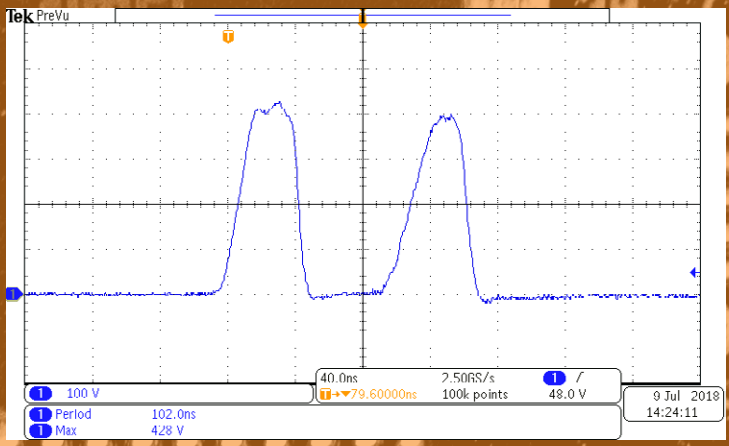
CW521 BALLISTIC GEL

What is the difference between a 4 mm probe and a 1 mm probe? What if you are using your own custom probe geometries? How much resolution can we achieve on positioning? Ballistic Gel helps answer those questions - it provides a stand-alone large SRAM chip, onto which a data pattern is loaded. Inject a fault, and then compare how the pattern is corrupted.



PROBE MONITORS

We don't want you driving blind. So our oscilloscope monitor ports provide an output that works directly with your regular oscilloscope, and lets you monitor the injected waveform.



CHIPWHISPERER + CHIPSHOUTER

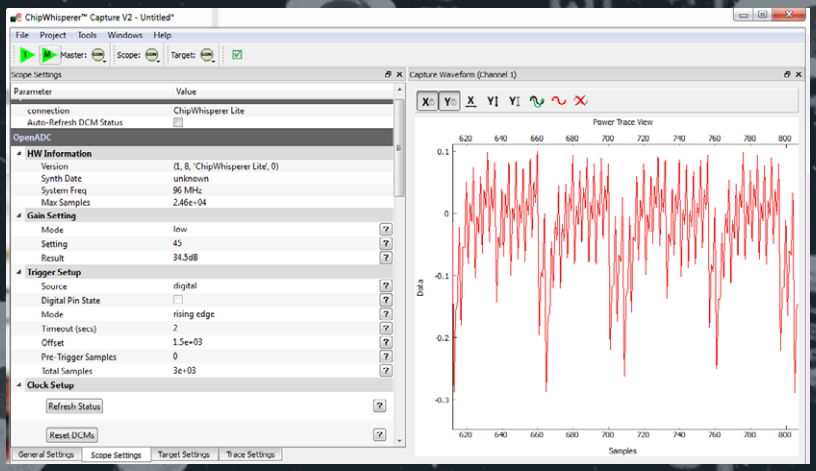
Use the ChipWhisperer to trigger fault injection, allowing you to combine power analysis + fault injection. Or use features like the analog pattern matching in the ChipWhisperer-Pro to trigger a fault based on certain patterns.

Simple EMFI Target provides quick visual feedback on device operation and fault injection.

OPEN-SOURCE PROJECTS

ABOUT THE CHIPWHISPERER HARDWARE & SOFTWARE

The ChipWhisperer project is an open-source toolchain for embedded security research. All of the targets and capture hardware in this catalog are supported by a Python-based capture application. The open-source nature means you can modify for your specific needs – whether you are developing your own algorithms or want to perform validation on a proprietary targets, ChipWhisperer has you covered.

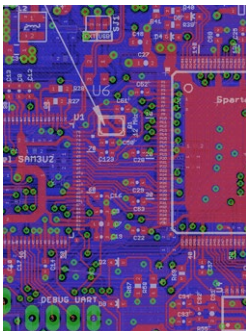


OPEN SOURCE HARDWARE

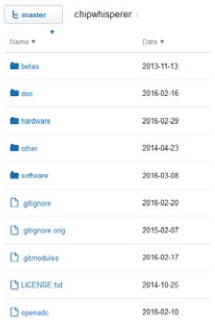
ChipWhisperer-Lite has *full* design files available (Schematics, PCB, FPGA, Firmware, BOM) with permissive licensing. *Most* products have schematics, FPGA designs, and firmware available to be modified for user-specific applications.

OPEN SOURCE SOFTWARE

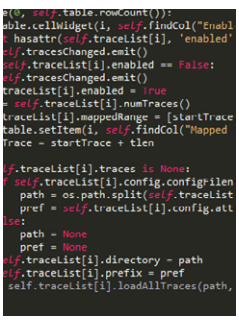
Capture and analyzer application is fully open source. Captured traces can be written to a variety of formats, including NumPy and MATLAB for use with existing codes. Proprietary modules can be inserted into open-source firmware.



FULLY OPEN-SOURCE

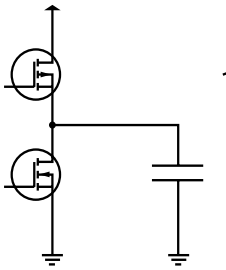


PUBLIC GIT REPO



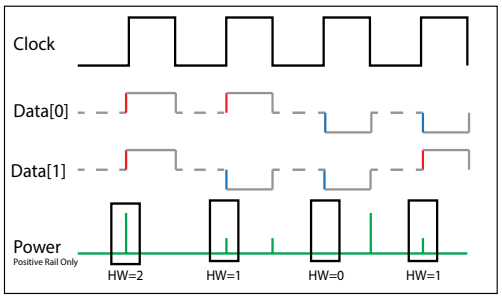
PYTHON SOURCE

POWER ANALYSIS



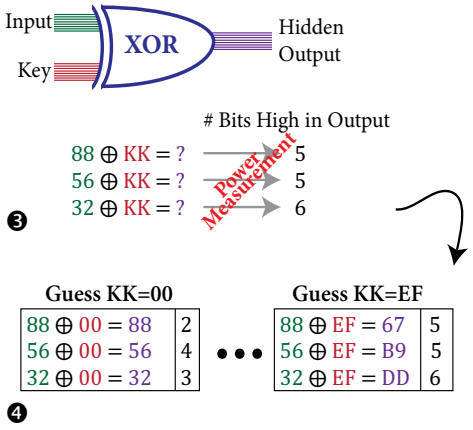
Digital Devices use electronic switches to drive bus lines high (VCC) or low (GND). This is equivalent to driving a capacitor to VCC or GND.

❶



The data lines are typically driven to a 'precharge' state half-way between VCC and GND. By looking at the power usage, we can determine how many bits were set to '1' vs '0' on every clock edge.

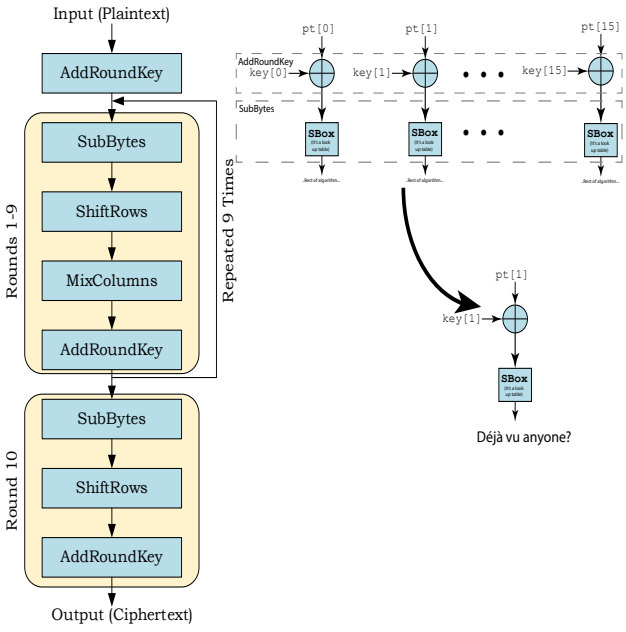
❷



Power analysis takes advantage of physical leakages on the device. We can see that different data causes small changes in power consumption. Using a "guess and check" algorithm (step ❹), we can look for the best match between the physical power measurment that occurred with known (public) data, and unknown secret key. We use a metric (such as correlation) to provide us with a way to rank how closely our model (❸) matched the physical measurements.

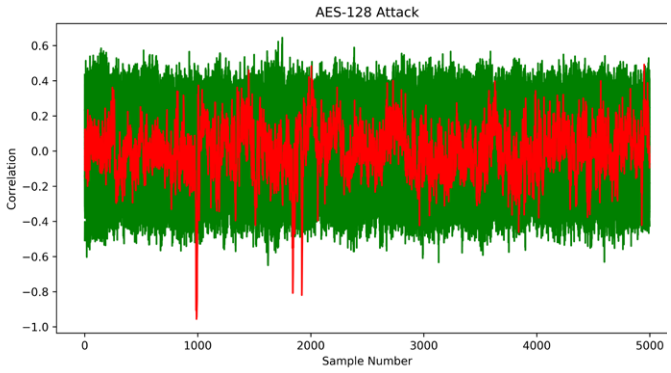
SURELY AES-128 IS SECURE...

AES (including AES-128, AES-192, and AES-256) is fundamentally designed to process data in a byte-wise order, and performs this "key XOR input" operation we just discussed. This applies to all unprotected implementations - be it 32-bit with T-Table, hardware processing 128-bits on one clock cycle, and everything in-between.



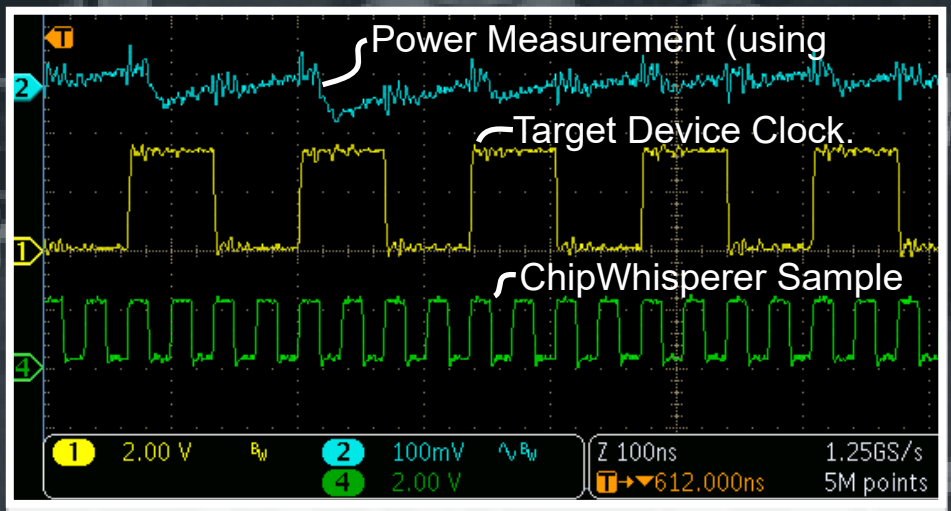
CORRELATION RELATION

After monitoring only fifty encryption operations on a STM32F3 running at 7.37 MHz, here is a plot of every wrong key-guess (in green) along with the correct key-guess (in red). Note there is a strong correlation only with the **correct key guess** and this correlation peak happens only at a **specific moment in time**. This attack does not require us to have precise timing on the crypto-graphic operation location, since the attack itself discovers this.



SYNCHRONOUS ARCHITECTURE

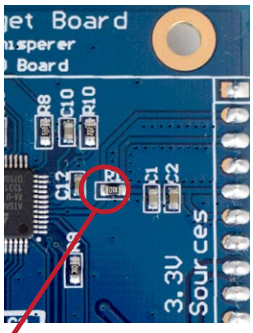
Our synchronous architecture means the power measurements, glitch locations, and triggers are always cycle-accurate with the reality of the hardware you are running on. It's what makes NewAE Technology Inc.'s products different from standard test gear.



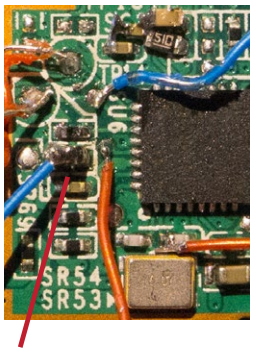
Our ChipWhisperer capture hardware can use a target device clock and apply multiplications and phase shifts to sample at desired point(s) during the clock cycle.

MEASURING EMISSIONS

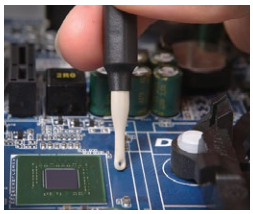
MEASURING THE POWER INFORMATION CAN HAPPEN IN A FEW POSSIBLE WAYS:



Custom target boards can be built with shunt resistors built in for low-noise measurements.



Shunt inserted into power supply. Addition I/O lines such as clock and serial tapped off.



A changing current generates a changing magnetic field. We can pick this up using H-Field probes, avoiding the requirement to modify the target board.

CLOCK GLITCHING

RUNNING OUT OF SPEC FOR FUN & PROFIT

C Code

```c
int checkpassword(char * inp){
    char knownpasswd[] = "touch";
    int passok = 1;

    //Check Password, avoid Timing Attacks
    //By always checking all characters!
    for(cnt = 0; cnt < 5; cnt++){
        if (inp[cnt] != passwd[cnt]){
            passok = 0;
        }
    }

    return passok;
}
```

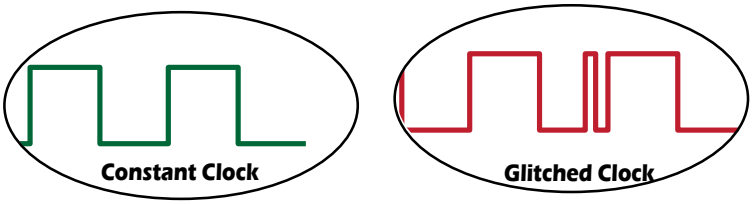
ASM Code

```
...
cpse  r25, r24
ldi   r20, 0x00
subi  r18, 0xFF
cpi   r18, 0x05
brne
...
```

Regular code execution uses a **constant clock** to step through a single instruction at a time.

Glitches in the clock mean the microcontroller begins executing an instruction, but before this is finished another clock edge arrives, and the next instruction is executed. We've effectively **skipped** an instruction.

If this instruction is part of a **password check** or other authentication, we can skip authentication completely!



FUSE BYTES

Fuse bytes protect your critical code. But often they are just stored in flash memory and checked by boot ROM - glitching this check could unlock even a "disabled" chip!

el	Flash Value	JTAG/SWD	Serial Bootloader
ISP	0x4E697370	Enabled	Disabled
1	0x12345678	Disabled	Subset of commands (read disabled)
2	0x87654321	Disabled	Subset of commands (read disabled)
3	0x43218765	Disabled	Disabled. Claimed impossible to recover
alid	Any other value	Enabled	Enabled

This example chip is especially vulnerable to glitching - causing any invalid value to be loaded will completely disable code protection.

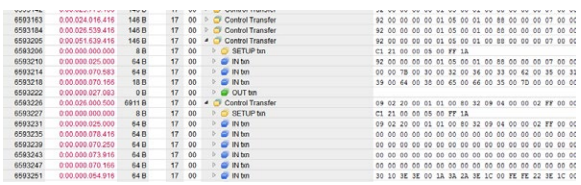
SIGNATURE CHECK

You can use the most secure signature verification in the world, but at some point you have to make a decision about the validity. This decision point will be a tempting target for fault injection attacks!

```c
sig_ok = validate_firmware(fw_ptr);
if (sig_ok){
  //Signature OK
  erase_flash();
  program_app();
  jump_to_app();
}
```

USB READ REQUEST

A common feature of USB stacks is to send back the minimum of the requested size OR data structure size. But what happens when we glitch this code:

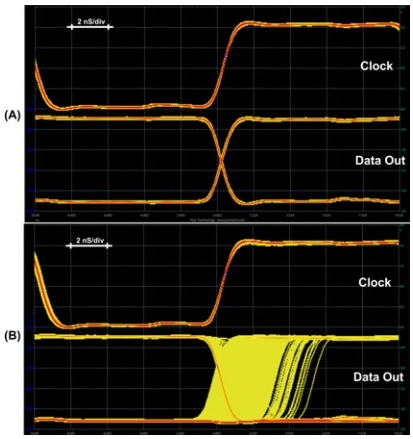


FAULT INJECTION METHODS

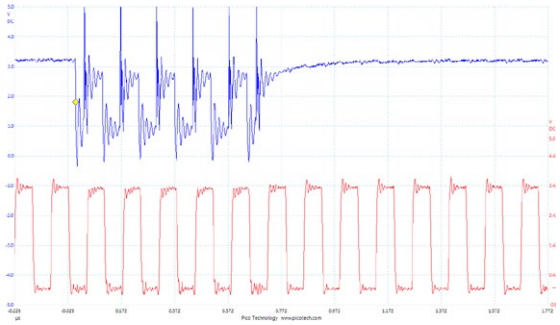
Violating the setup & hold times of flip-flops (registers) is one example of a fault injection method. This can cause metastability in the internal flip-flops - the figure on the right shows an example of a metastable propogation (A) compared to a normal propagation through the flip-flop (B). This results in incorrect data being moved through a databus.

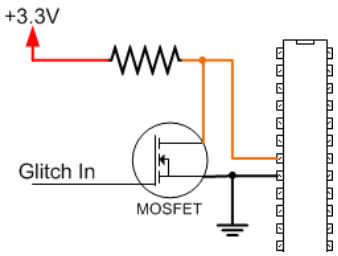
The ChipWhisperer-Lite and -Pro include a number of timing circuits to generate very precise glitchy clocks, to trigger these types of events.

We can also trigger similar effects through voltage glitching.



VOLTAGE FAULT INJECTION

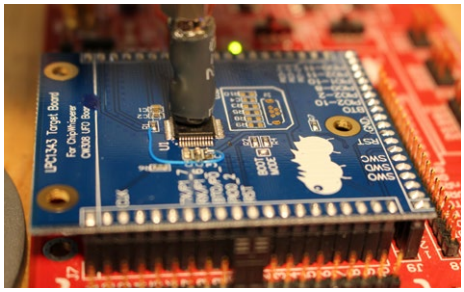




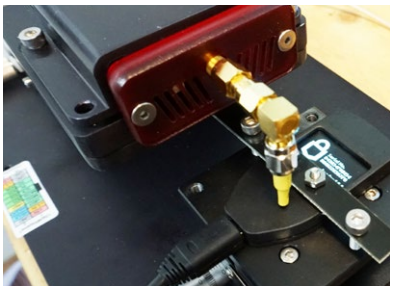
A crowbar (built into ChipWhisperer) is a low-cost and effective method of generating faults using voltage fault injection. It can be used with external targets easily as well.

ELECTROMAGNETIC FAULT INJECTION (EMFI)

Our end goal is to induce voltages inside a target device. We can use a coil (like the one above) to generate a short powerful EM pulse by sending a short high-voltage pulse through the coil. The higher voltage helps us generate a sufficiently high di/dt even with a reasonable coil inductance.



We can position this coil over a target chip. It requires very precise positioning, necessitating some sort of jig or XY table. But it also means we gain another dimension of control of our glitch - not just time and power, but also XY location. This glitch can cause all the effects detailed on the fault injection background panel.



We can even insert EM glitches through a device enclosure when chips are near the surface of the device! Above an EMFI works against a bitcoin wallet.

CHIPWHISPERER TRAINING

OCT 5-8TH & 12-15TH - LIVE ONLINE BY HANDSONTRAINING

Advanced Hardware Hacking with the ChipWhisperer: Hands-On Side Channel Analysis, Fault Injection and Their Countermeasures (4 days)

See **www.handson-training.com/page/Advanced-Hardware-Hacking-with-the-ChipWhisperer**

NEWAE ONLINE TRAINING - CHIPWHISPERER.IO

Learn the ultimate combination of theory, hands-on labs, and application-specific examples to give you an invigorating embedded security training through our online courses.

See **http://learn.chipwhisperer.io**

FIND MORE DETAILS AT NEWAE.COM/TRAINING

NewAE Technology Inc.
1083 Queen St., Suite 196
Halifax, N.S. B3H 2R8
Canada

sales@newae.com
www.newae.com
ph: +1 902 999 8869

Visit NewAE.com for more information!