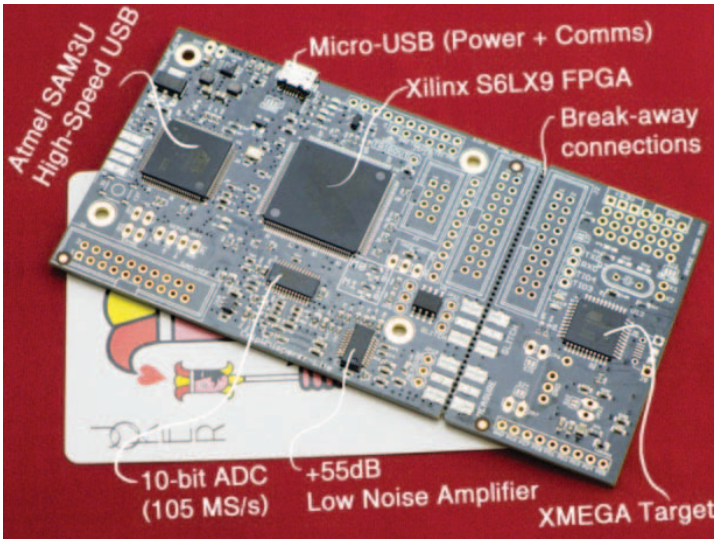
NewAE Technology Inc.
newae.com

ChipWhisperer® Embedded Security Analysis Tools
Capture Hardware

CW1173: ChipWhisperer-Lite

Product Datasheet



The ChipWhisperer-Lite represents NewAE Technology Inc.'s most aggressive pursuit of it's mission to bring side-channel power analysis and glitching attacks to every engineer and student. The FULLY open-source (hardware, software, firmware, FPGA code) is launching a revolution in hardware security.

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. The single-board version comes in two variants: Atmel XMEGA or STM32F3 Arm target.

You can break apart the capture & target side to connect to other targets. The capture portion is available standalone which comes ready with SMA & target connectors, but requires an external target.

Product Highlights

10-bit ADC with 105 MS/s sampling rate combined with up to +55 dB gain amplifier measures small signals easily.

Advanced synchronous clock locking logic samples target power on related clock edges, drastically reducing sample rate requirements compared to power analysis performed with regular oscilloscopes.

Clock and voltage fault injection possible using FPGA-based pulse generation.

Single-board solution ideal for teaching and training environments, and design of boards allows easy separation of target for future expansion.

Programmers for XMEGA (PDI) and STM32Fx (serial bootloader) targets built in, meaning no external equipment required.

Ordering Summary

NewAE Part Number	Target Processor P/N	Form Factor	External Connections
NAE-CWLITE	ATXMEGA128D4	Single Board	USB
NAE-CWLITE-ARM	STM32F303RCT7	Single Board	USB
NAE-CWLITE-CAPTURE	None	Single Board	USB, SMA (Capture + Fault), 20-pin cable
NAE-CWLITE-2PART	ATXMEGA128D4	Two Boards	USB, SMA (Capture + Fault), 20-pin cable

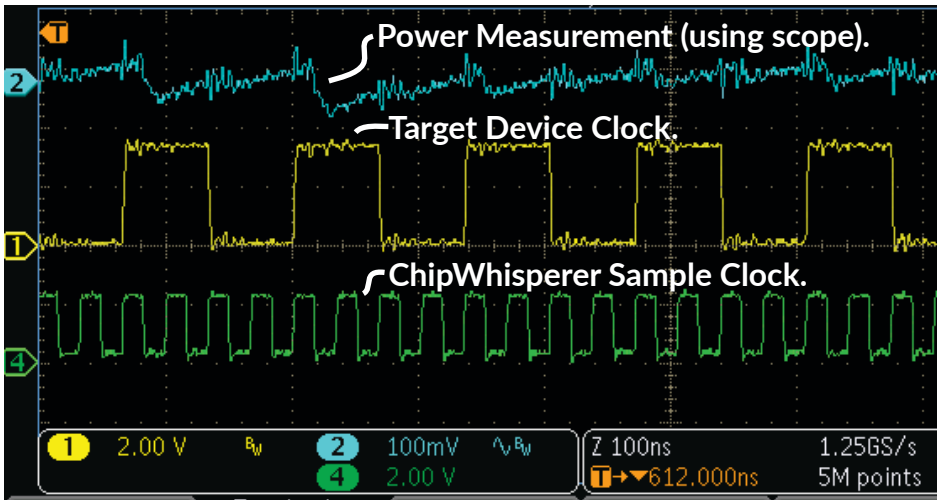
Product Links

Full Documentation	https://wiki.newae.com/CW1173_ChipWhisperer-Lite
Tutorials and Examples	https://wiki.newae.com/
Design Files	https://github.com/newaetech/chipwhisperer/tree/master/hardware/capture/

Specifications

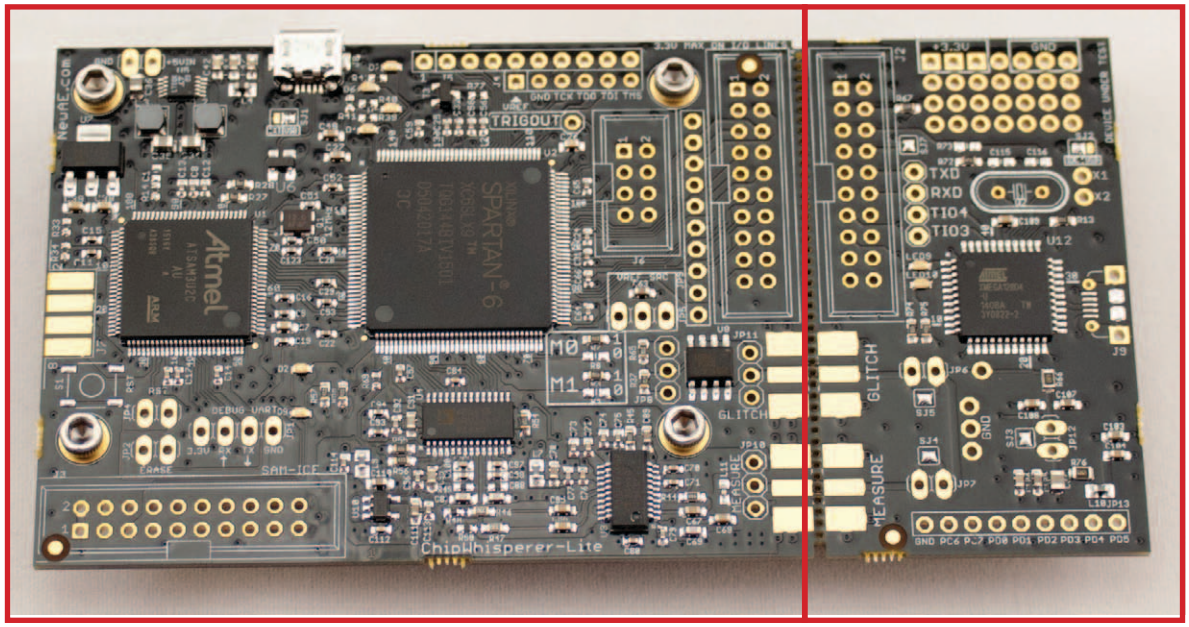
Feature	Notes/Range
ADC Specifications	10-bit ADC, 105 MS/s maximum sample rate.
ADC Sample Clock Source	Internal generator, external input (direct or with 4x multiplier or phase adjuster).
Analog Input	AC-Coupled, up to +55dB adjustable gain.
GPIO Types	Serial, clock, logic line (i.e., for reset pin).
GPIO Voltage	3.3V.
Clock Generation Range	5-200 MHz.
Clock Output Type	Regular, with glitch inserted, only output glitch.
Glitch Width (min)	~4nS (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). STM32F303RCT7 on Arm variant.
Programming Protocols	Atmel ISP (for AVR), Atmel PDI (for XMEGA), STM32Fx Bootloader

Synchronous Architecture



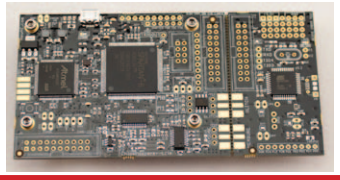
Our ChipWhisperer capture hardware can use a target device clock and apply multiplications and phase shifts to sample at desired point(s) during the clock cycle. This ensures sample points are directly related to the digital clock which generates the signals of interest. The result is many devices can be successfully attacked with 5-100x slower sample clock compared to a regular oscilloscope.

Detailed Ordering Information

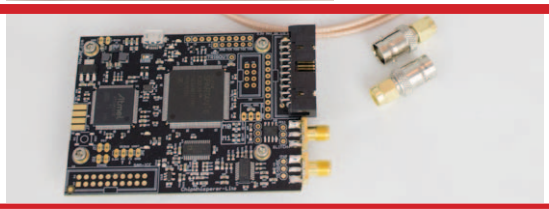


CAPTURE Section TARGET Section

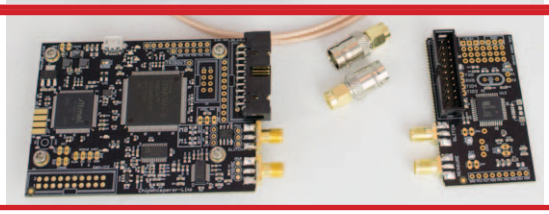
NAE-CWLITE & NAE-CWLITE-ARM: The the CAPTURE and TARGET sections are on one unbroken board. Includes a USB cable.



NAE-CWLITE-CAPTURE: Includes the CAPTURE only. Also includes 2x SMA cables, 2x SMA to BNC adapters, and a 20-pin cable.

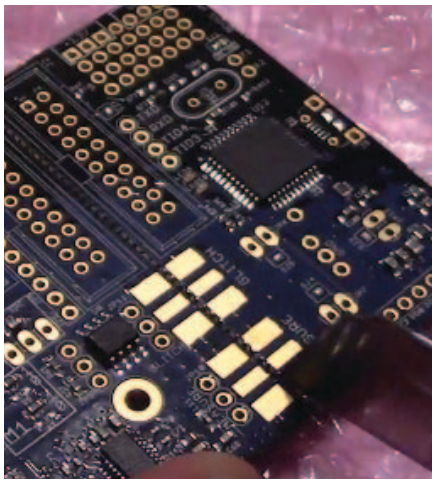


NAE-CWLITE-2PART: Includes the CAPTURE & TARGET separately (only XMEGA target). Also includes 2x SMA cables, 2x SMA to BNC adapters, and a 20-pin cable.

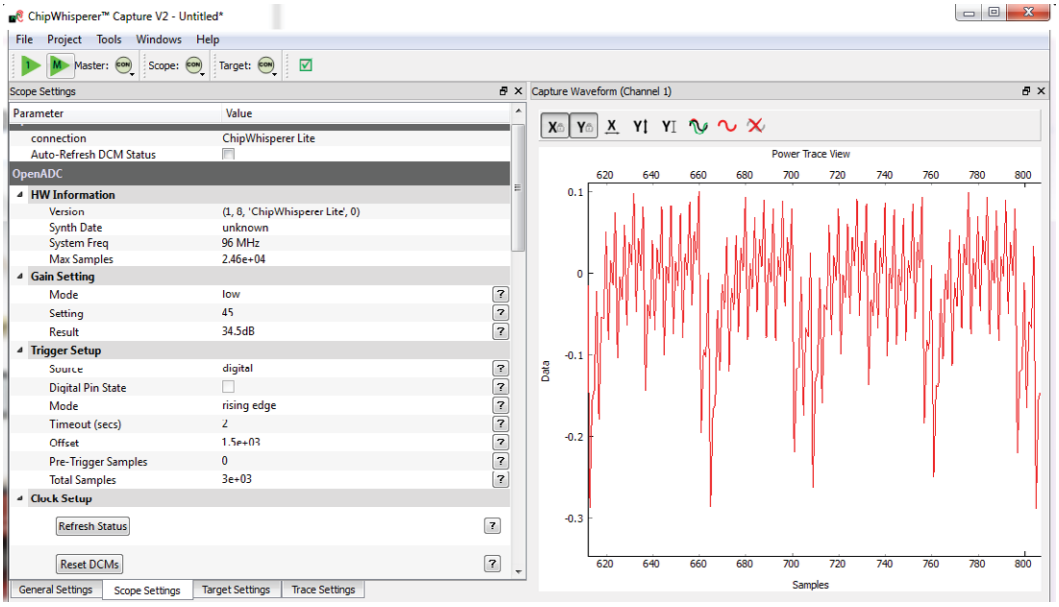


Single or Dual Board?

- The single-board version (NAE-CWLITE & NAE-CWLITE-ARM) 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 does not include a target.
- The -2PART version has the devices split apart such you reconnect them with provided SMA and 20-pin IDC cable.
- It's always possible to "break" the single-board version apart.



Software Support



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.

ChipWhisperer runs on most computer platforms (Windows, Mac, Linux). You can freely download and use the open-source software to confirm functionality.

Disclaimers