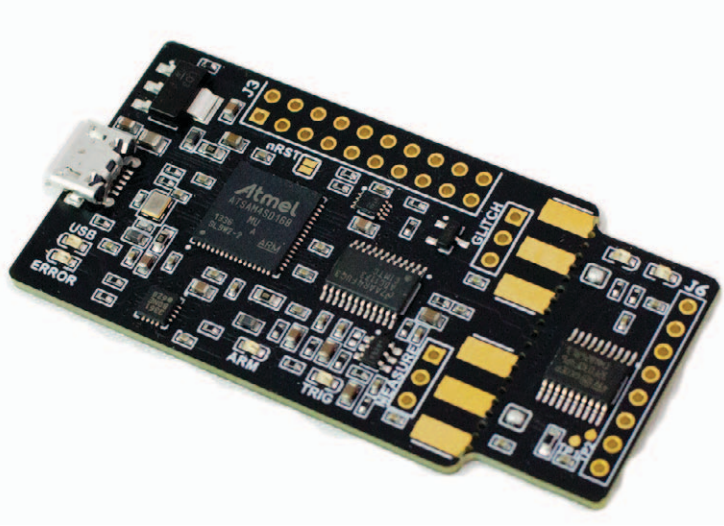
NewAE Technology

NewAE Technology Inc.
newae.com

ChipWhisperer® Embedded Security Analysis Tools
Capture Hardware

CW1101: ChipWhisperer-Nano

Product Datasheet



The ChipWhisperer-Nano is the lowest cost platform for performing side-channel power analysis attacks in training and educational environments. This device has a smaller subset of features compared to the ChipWhisperer-Lite or -Pro, but still allows you to perform many of the tutorials and demos.

The use of synchronous sampling ensures that this low-cost device can be used for performing real power analysis of algorithms and devices. The built-in target is a STM32F030F4P6 which has 16KB of FLASH and 4KB of SRAM.

It is possible to cut the included target off and attach to external targets, such as the CW308 base-board. This allows an external clock to be routed to the on-board ADC for measuring of external devices.

Product Highlights

8-bit ADC with 20 MS/s sampling rate and fixed-gain front-end allows measurements of on-board and some external targets.

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.

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

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

Note this platform has limited VCC-glitching capability and no clock glitching capability, instead primarily focusing on side-channel power analysis.

Ordering Summary

NewAE Part Number	Target Processor P/N	Form Factor
NAE-CWNANO	STM32F0	Single Board with micro-usb cable
NAE-CWNANO-LEARNIN	STM32F0	Classroom Pack of 20 boards + micro-usb cables

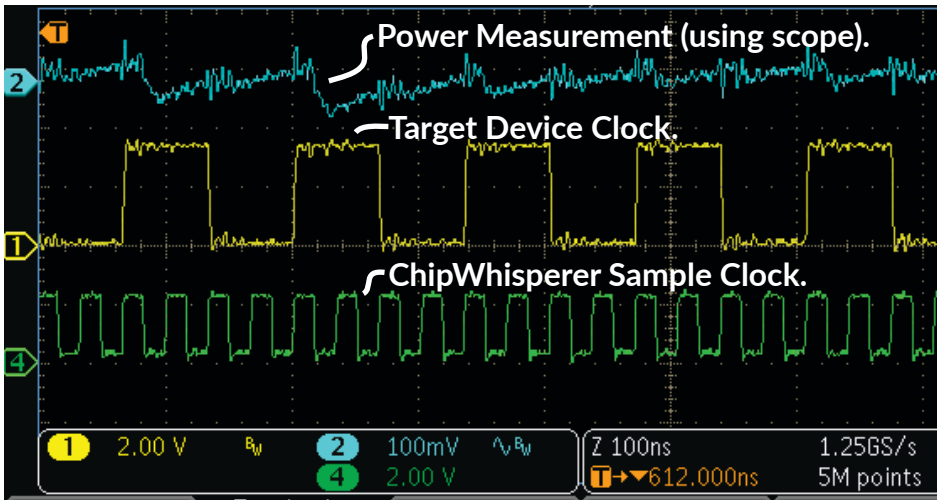
Product Links

Full Documentation http://wiki.newae.com/CW1101_ChipWhisperer-Nano
Tutorials and Examples https://wiki.newae.com/

Specifications

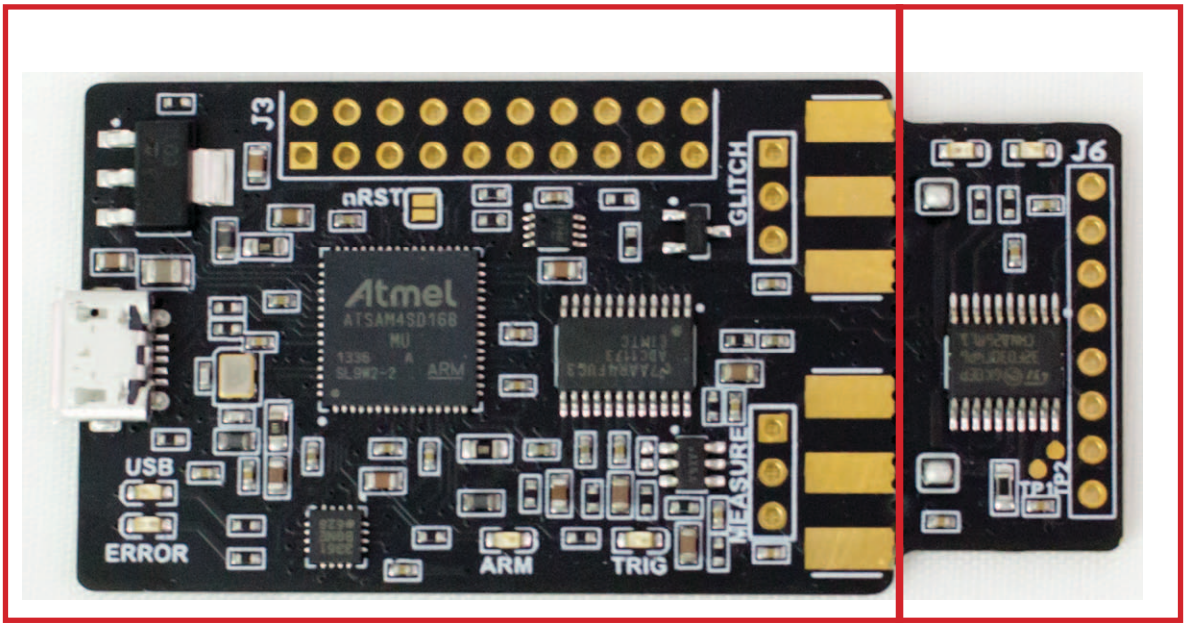
Feature	Notes/Range
ADC Specifications	8-bit ADC, 20 MS/s maximum sample rate.
ADC Sample Clock Source	Selectable between internal generator or external input.
Analog Input	AC-Coupled, fixed gain.
GPIO Types	Serial, clock, logic line (i.e., for reset pin). Fixed pin functions.
GPIO Voltage	3.3V.
Clock Options	3.75 MHz, 7.5 MHz, 15 MHz, 30 MHz , 60 MHz
Clock Output Type	Generated by microcontroller, clock only (no clock glitching support).
Trigger Type (ADC + Glitch)	Rising edge only.
Glitch Width (min)	~20nS (depends on cabling used for routing glitch output).
Glitch Offset	~200nS jitter, adjustable in 10nS increments.
Voltage glitch type	Low-power crowbar circuitry.
Crowbar pulse current	4A.
USB Interface	Custom USB firmware (full-speed USB 2.0 device).
Sample Buffer Size	50 000.
Target Device	STM32F030F4P6 or STM32F070
Programming Protocols	STM32Fx Bootloader

Synchronous Architecture



Our ChipWhisperer capture hardware can use a target device clock 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

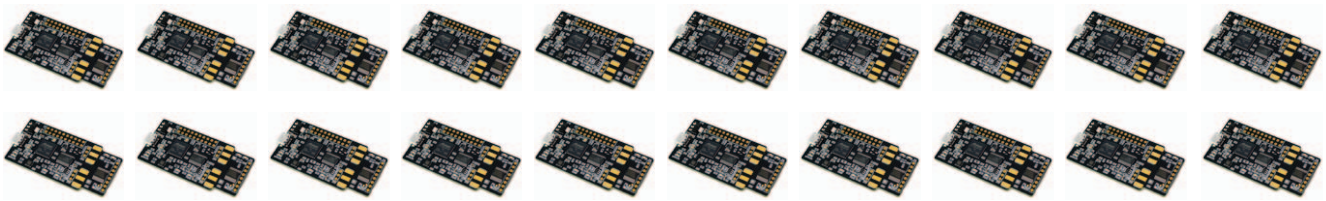
Our ChipWhisperer-Nano follows the same idea of the ChipWhisperer-Lite, providing a low-cost platform including both the measurement and target on one board. But it does away with the FPGA to reduce cost to a bare minimum - the result is a board that can be used for teaching workshops and classes, while still providing students with hardware they can keep.

The target section can be broken away for attacking real targets, best done by using this in combination with our CW308 UFO board system.

Note the ChipWhisperer-Nano has no clock glitching support and limited voltage glitching support, mainly because the glitching is not generated in a dedicated FPGA hardware resource like the ChipWhisperer-Lite or -Pro.

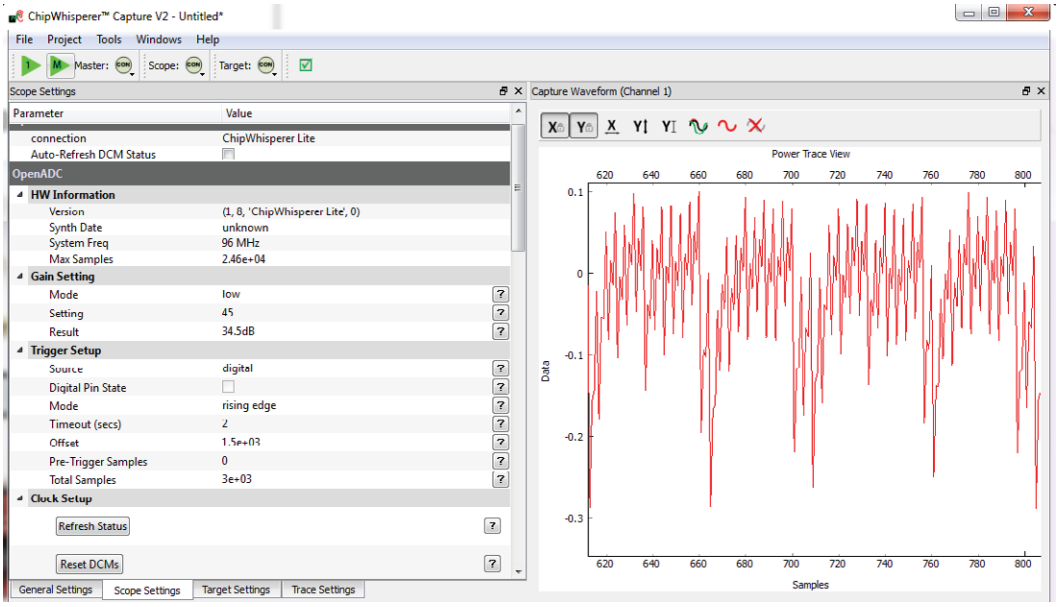
Classroom Pack?

To better equip your classroom or training, you can use the product code "NAE-CWNANO-LEARNIN". This includes 20 devices at a lower per-device cost, all in one handy box.



NAE-CWNANO-LEARNIN

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

This product may be protected by U.S. patent no. 9,429,624; 9,523,737. NewAE is part of the Open Patent Non-Assert pledge. See newae.com/patent for more information.

NewAE Technology makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. NewAE Technology does not make any commitment to update the information contained herein. NewAE Technology products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life. NewAE Technology products are designed solely for teaching purposes.