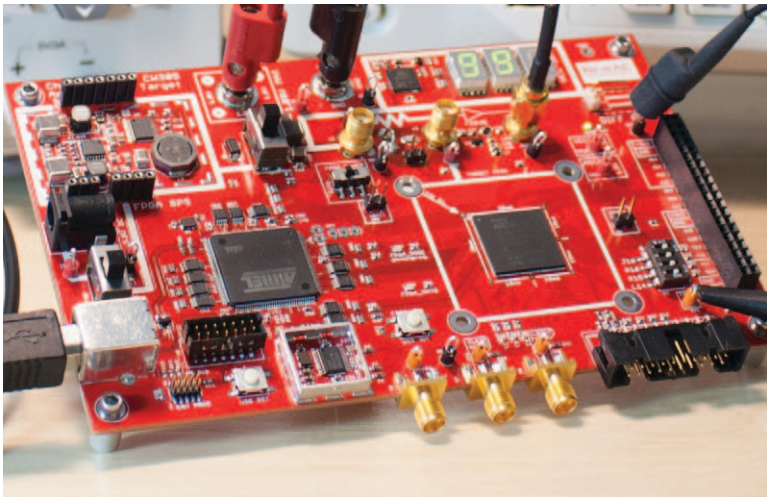
NewAE Technology Inc.
newae.com

ChipWhisperer® Embedded Security Analysis Tools
Stand-Alone Targets

CW305 Artix FPGA Target

Product Datasheet



The CW305 is an advanced target for performing power analysis & fault injection attacks against hardware cryptographic functions implemented in 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.

Product Highlights

Shunt resistor for measurement of power consumption of core implemented on FPGA. Default option of no decoupling capacitors mounted leaves high-frequency signals present across shunt.

ESD protection reduces possibility of resetting USB interface when inserting EM or voltage faults.

Three types of FPGA targets (-A35, -A100, SOCKET) allowing implementation of large cryptographic cores.

Custom USB interface provides simple address/data register set leaving you to concentrate on FPGA core, and not on details of the USB Interface protocol.

Programmable VCC-INT power supply & external oscillators allow you to control external parameters over USB for validation across voltage and frequency.

Ordering Summary

NAE-CW305-04-☐-☐-☐

- ☐ Decoupling capacitor options
- ☐ Shunt resistor
- ☐ FPGA type

Product Links

Full Documentation	http://cwdocs.com/cw305
Example FPGA Projects	https://github.com/newaetech/chipwhisperer/tree/master/hardware/victims/cw305_artixtarget

Specifications

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).

Detailed Ordering Options

Revision (04)
Revision normally omitted from ordering codes.

NAE-CW305-04-7A35-0.10-X

Shunt value (ohms)

Code	Shunt	Notes
0.1	100 mOhm	Default & recommended value for most uses.
0.0	0 mOhm (jumper)	Useful for EM probe measurements or PUF usage.

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.

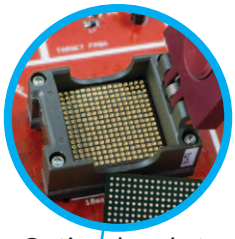
Code	PDN	Notes
X	No VCC-INT Capacitors	The decoupling capacitors on the VCC-INT network are NOT present. This option is required if performing side-channel power analysis using the current shunt.
M	VCC-INT Capacitors	The decoupling capacitors on the VCC-INT network are present. Generally if using the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

Board Features

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.



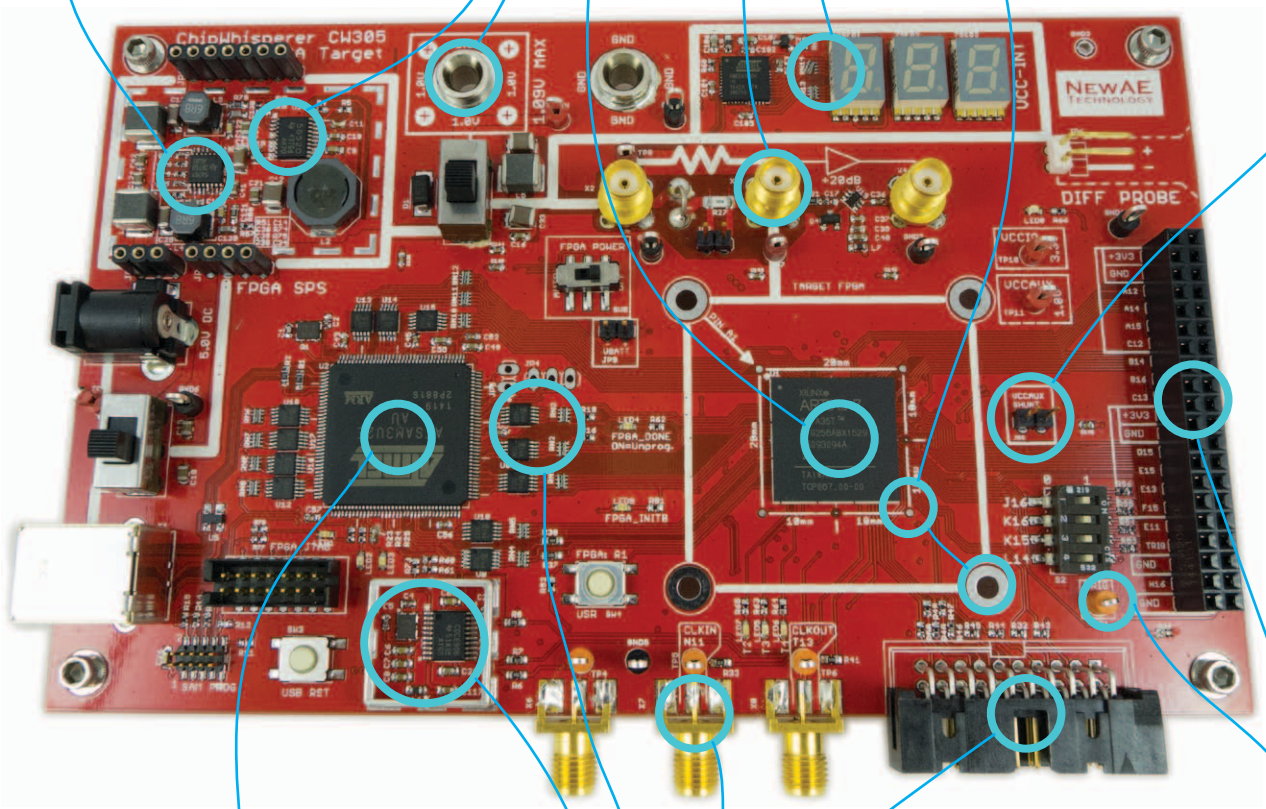
Optional socket available.

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.

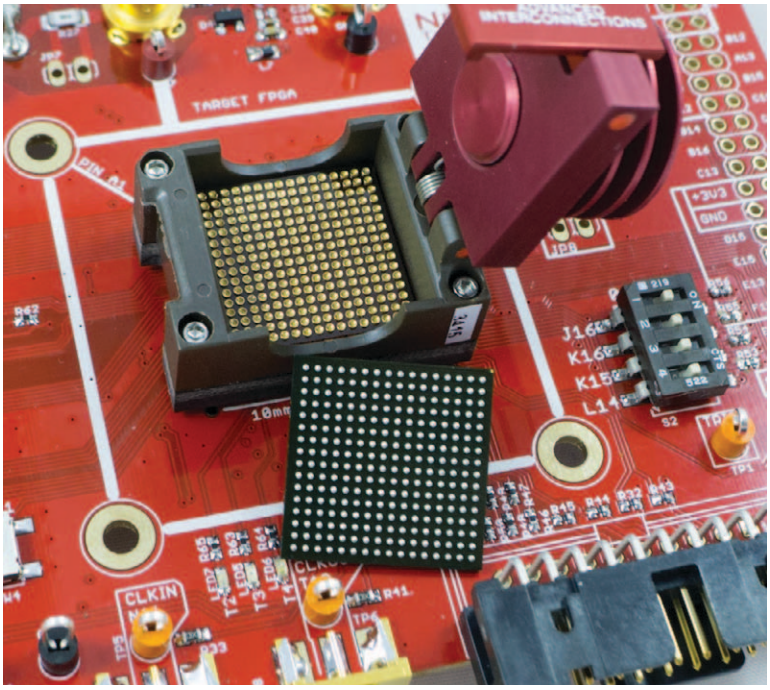
Expansion header for additional I/O.

20-Pin Connector for ChipWhisperer capture hardware.

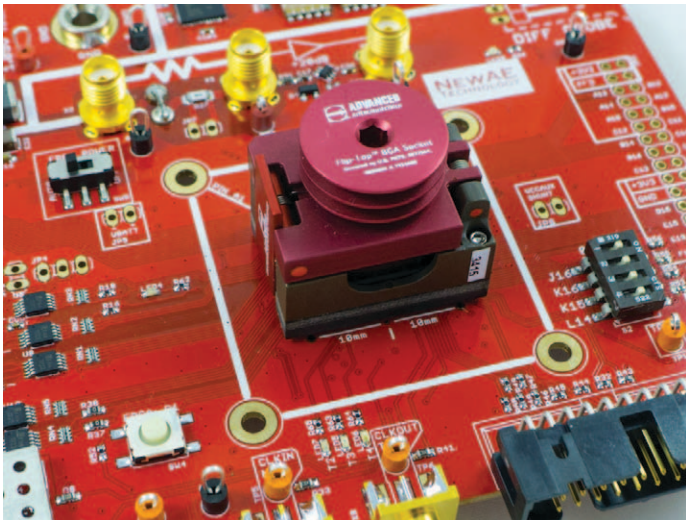
SMA connectors for clock input/output.

Socket Usage

Boards ordered with the SOCKET option contain a BGA socket. The following shows a FPGA (upside down) next to the open socket:

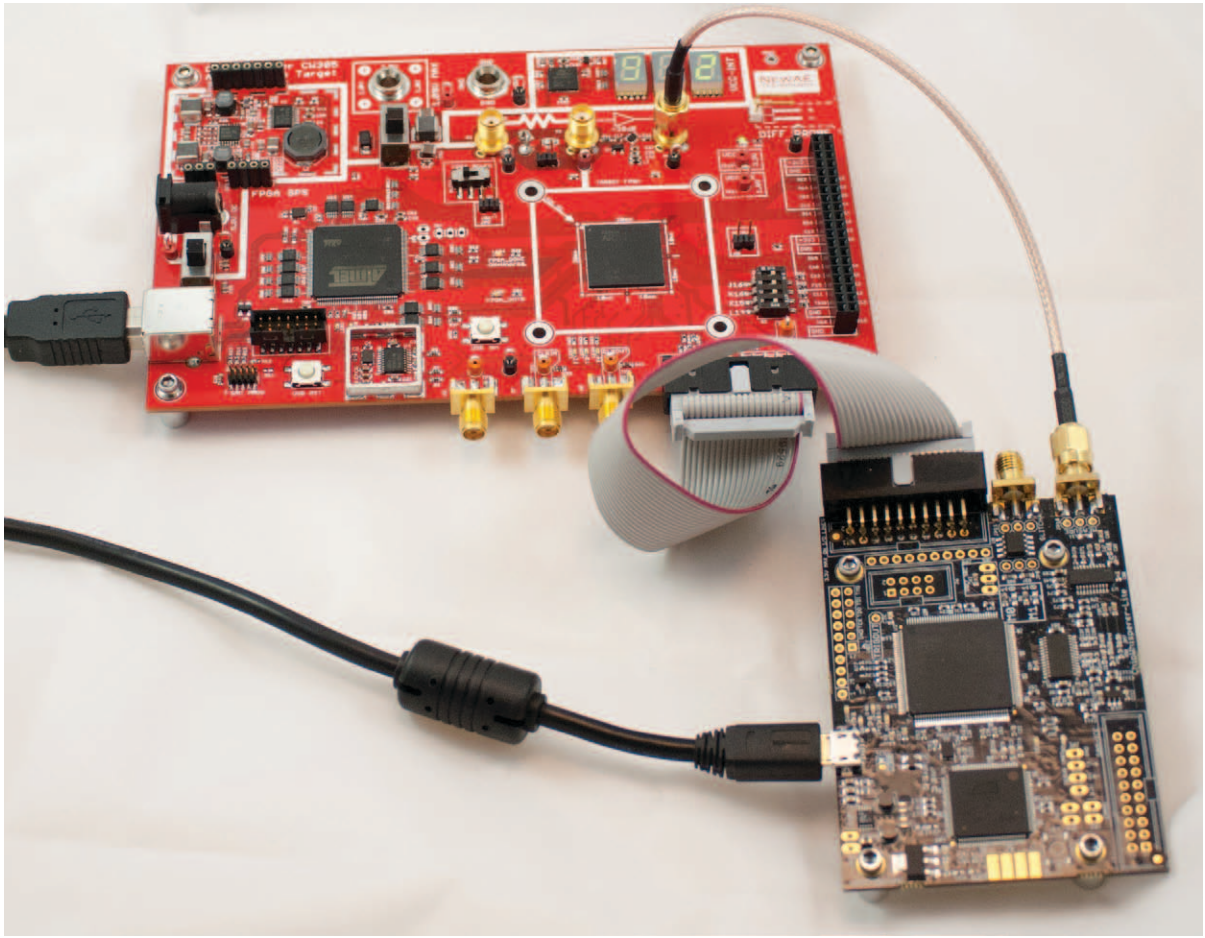


When closed, the socket has a heat sink on top of the FPGA. Note the socket prevents usage with an EM probe or similar.



The socket can fit any Artix 7 device in the FT256/FTG256 package. Currently this means the following devices are supported: XC7A15T, XC7A35T, XC7A50T, XC7A75T, XC7A100T. If ordering an FPGA for the socket ensure it is in the FT256/FTG256 package. Note the 'G' package indicates usage of lead-free (Sn/Ag/Cu) solder balls, whereas the FT256 package uses Sn/Pb solder balls. Either walls will work with the BGA socket.

ChipWhisperer Capture Usage



The CW305 can be used with the ChipWhisperer Capture hardware (either CW1173 or CW1200). The ChipWhisperer capture hardware provides power analysis, along with clock and voltage glitching. This forms a complete low-cost and standalone lab that does not require any additional test equipment such as oscilloscopes or power supplies.

See the wiki (at ChipWhisperer.com) for full details and example tutorials of this product.

Disclaimers