ABV-IIITM Gwalior

Ref:ABV-IIITMG/Reg/2025/579 Date: **20/06/2025**

Notice for Inviting Quotation **(Second Call)**

Sub: Quotation for Supply of Chip Whisperer Side-Channel Analysis Tool Kit

1. Quotations are invited in sealed cover for the supply of Side-Channel Analysis (SCA) Tool Kit, CW308 UFO Target boards and accessories with the following features:
   - ChipWhisperer-Lite 105 MS/s ADC with adjustable gain
   - Perform side-channel power analysis, voltage fault injection, or clock fault injection.
   - CW308 UFO Board features low-noise power supplies, probing points, and connectors to simplify usage.
   - Targets: XMEGA 8-bit RISC, STM32F0 Cortex-M0 and, STM32F3 Cortex-M4.
   - Probe set including magnetic-field (H-field) and differential probe with isolated power supply.
   - Level shifter for interfacing to external targets.
   - Other targets for CW308 UFO Board [Targets List and their specifications given below]
   - OpenOCD as an external JTAG/SWD programmer compatible with the EFR32MG21A Target for CW308.

   You are requested to submit the competitive rates as per the specification below.

Sr. No.	Item Description	Qty.	Total Amount
1.	ChipWhisperer Level 2, SCA Tool Kit (ChipWhisperer-Lite, CW308 UFO Board, with one XMEGA and two STM Targets, Probe set including magnetic-field and Level Shifter)	01	
2.	CW308 UFO Target boards [List given below]	13	
3.	OpenOCD	01	

2. **Specifications for ChipWhisperer SCA Level 2 Kit:**

ADC Specifications	10-bit ADC, 105 MS/s maximum sample rate
ADC Sample Clock Source	(1) Internal generator, (2) External input direct, (3) External input with phase adjustment, (4) External input with 4x multiplier, phase adjustment
Analog Input	AC-Coupled, up to +55dB gain (adjustable)
Trigger Sources (Glitch & ADC)	Rising/Falling Edge, Level
GPIO Types	Serial, clock, logic line (i.e., for reset pin)
GPIO Voltage	3.3V
Clock Generation Range	5-200 MHz
Clock Output Type	(1) Regular, (2) with glitch inserted, or (3) glitch output only
Glitch Width (min)	~1nS (depends on cabling used)
Glitch Offset	Adjustable in < 200pS increments
Crowbar pulse current	20A
USB Interface	Custom open-source USB firmware, up to 25 MB/s speed
Sample Buffer Size	24 573
Programming Protocols	Atmel ISP (for AVR), Atmel PDI (for XMEGA), STM32Fx Bootloader
Connectors	Power Measurement In: SMA, Crowbar Glitch Out: SMA, Target Connector: IDC-20

3. Package List of ChipWhisperer SCA Level 2 Kit:

Item	Details	Qty
STM32F3 UFO Target	STM32F303 Target for CW308 UFO	1
5V DC 2.1mm barrel jack wall-wart	Power Supply for UFO Board (only required for 5V targets)	1
CW506 Advanced Breakout Board	Level shifter with additional connections for external targets.	1
7.3728 MHz Crystal	Crystal for using UFO Board stand-alone	1
Differential Probe	Differential probe, +/-5V input range	1
Prototyping UFO Target Boards	Prototyping boards for CW308 UFO	3
Low Noise Amplifier	20 dB Low Noise Amplifier, Unshielded	1
Isolated Probe Power Supply	Isolated power supply for differential & LNA/H-Probe	1
5V DC USB Wall-wart	Wall adapter for Probe USO Power	1
SMA Coupler	SMA Coupler for connecting H-Probe to LNA Input Directly	1
STM32F0 UFO Target	STM32F071 Target for CW308 UFO	1
UFO Lifter Tool		2
XMEGA UFO Target	XMEGA Target for CW308 UFO (Mouted on UFO Board)	1
6-pin Ribbon/IDC Cable	Power cable for LNA & Diff-Probe	3
SMA to BNC Adapter	SMA to BNC Adapter, for probes or instrumentation	2
Planar H-Field Probe	Magnetic Field Probe, 15mm loop, Planar, Stubby	1
SMA Tee	SMA Tee for performing DPA & voltage FI on UFO Board simultaneously	1
Micro-USB Cable (3 ft)	Micro-USB cable for ChipWhisperer-Lite	1
Micro-USB Cable (6 ft)	Micro-USB cable for Probe PSU Power	1
SMA Cables	Standard SMA cables	3
20-pin Ribbon/IDC Cable	20-Pin Ribbon Cable for Connecting between boards	2

4. CW308 UFO Target Board Lists and Their Specifications:

Sno	Board Name	Details	Target Chip	Architecture	HW Crypto	FLASH	SRAM
1	ATSAML11 Target for CW308	Arm Cortex-M23 core with hardware AES, includes DPA countermeasures outside the AES core, such as Hamming-Weight balanced RAM and FLASH access modes.	ATSAML11E16A	Arm Cortex-m23	AES	64 KB	16 KB
2	Spartan S6LX9 Target for CW308	Small FPGA target, Xilinx Spartan 6 LX9. Example AES implementation available.	XC6SLX9	FPGA - Spartan 6	User Defined	0KB	1430 Slices
3	LPC55S69 Target for CW308	Dual-Core Cortex-M33 core with PUF, AES hardware, and PRINCE memory encryption options. Supports special AES mode that reduces AES power signature.	LPC55S69JBD100K	Arm Cortex-m33	AES, RSA, PRINCE, SHA, SHA2	640 KB	320 KB
4	K82F Target for CW308	Arm Cortex-M4 core with two AES peripherals - one includes hardware masking DPA countermeasures.	MK82FN256VLL15	Arm Cortex-m4	AES, 3DES, RSA, ECC, SHA	256 KB	256 KB
5	STM32F2 w/ Hardware Crypto Target	STM32F2 series high-performance Arm Cortex-M3 device with hardware AES	STM32F215RET6	Arm Cortex-m3	AES, SHA1, 3DES, MD5, SHA	512 KB	132 kb

6	PSOC62 Target for CW308	Arm Cortex-M4/M0 dual-core device, with security features allowing Cortex M0 core to be used as boot device. Hardware AES peripheral.	CY8C6247BZI-D44	Arm Cortex-m4	AES, RSA, DES, SHA, ECC	1 MB	288 KB
7	EFR32MG21A Target for CW308	The EFR32MG21A board features the EFR32MG21A010F1024 from Silicon Labs. This device features a number of security features, including a dedicated “Secure Element” core that performs a secure boot operation, and DPA countermeasures on cryptographic primitives. Note: this board requires an external JTAG/SWD programmer (such as OpenOCD or J-Link) for use, as it does not include a bootloade).	EFR32MG21A	Arm Cortex-m33	AES, SHA, ECC	1 MB	96 KB
8	STM32L4 Target for CW308	STM32L4 high-performance series Arm Cortex-M4 device, includes hardware AES implementation peripheral.	STM32L443RCT6	Arm Cortex-m4	AES	256 KB	64 KB
9	D2000 Target for CW308	Intel Quark D2000 is a microcontroller using the x86 instruction set.	FND2000	X86	Not Present	32 KB	8 KB
10	ATSAM4L Target for CW308	Arm Cortex-M4 core with hardware AES that has four selectable DPA countermeasures.	ATSAM4LC2AA	Arm Cortex-m4	AES	128 KB	32 KB
11	STM32F4HWC Target w/ CANoodler bundle. Allows building demos using CAN peripheral of STM32F4 and hardware crypto.	CANoodler bundle with STM32F4HWC Target (which has CAN peripherals).	STM32F415RGT6	Arm Cortex-m4	AES, SHA1, 3DES, MD5, SHA	1 MB	192 KB
12	CEC1702 Target for CW308	Arm Cortex-M4 core with many cryptographic accelerators including AES, RSA, and ECC. No internal memory (uses SPI flash) makes development somewhat harder	CEC1702Q-B1-SX	Arm Cortex-m4	AES, SHA, SHA1, SHA2, ECC, RSA	0 KB	480KB
13	STM32F3 Target for CW308 with CANOODLER	CANoodler bundle with STM32F3 Target (which has CAN peripherals).	STM32F303RCT7	Arm Cortex-m4	Not Present	256 KB	40 KB

5. **Quotation (Terms and Conditions):**
    a. The price should be quoted on F.O.R. ABV-IIITM Gwalior delivery basis.
    b. The quotation should be valid for 30 days from the date of submission.
    c. The institute has the right to increase or decrease the number of quantity.
    d. All duties and other levies payable by the supplier under the contract shall beincluded in the unit Price.
    e. Applicable taxes, if any, shall be quoted separately.
    f. Payment after successful delivery, installation & configuration.
    g. Delivered licence should be perpetual in nature and warranty as per OEM.
    h. The quotations should contain the PAN, GSTIN number of the firm.

6. The last date for submitting the quotation is **30.06.2025** up to 5.00 PM. Any quotations submitted after the specified time and with incomplete information will not be accepted.

7. Sealed quotation (with "Quotations for Chip Whisperer Side-Channel Analysis Tool Kit" written on top of sealed envelope cover) to be submitted/ delivered at the address mentioned below,

The Registrar,
ABV-Indian Institute of Information Technology and Management Gwalior,
Morena Link Road, Gwalior,
Madhya Pradesh, India-474015