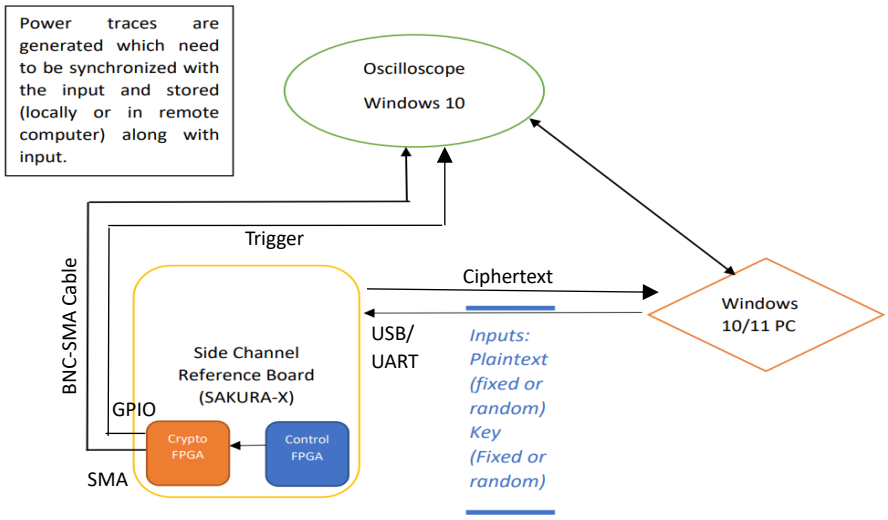
Side Channel Leakage Capture Mechanism Design, Implementation and SCA LAB Setup

1	**Problem Statement**	Side Channel Leakages Capture Mechanism Design, Implementation using SAKURA-X Board: Design and Implementation of side channel leakages capture setup for evaluation of cryptographic algorithms HDL strength implementation running on SAKURA-X crypto FPGA. The works includes: - - Synchronized side channel leakages traces capture scheme design using SAKURA-X and Oscilloscope along with corresponding plaintext and key. - Data I/O and Power/EM trace capture reference model development with AES 256 GCM HDL implementation. It includes development of I/O control PC software modules, SAKURA-X Control FPGA IP Cores and integration with C-DOT provided AES 256 GCM IP Core. - Trigger scheme design for Oscilloscope and captured traces alignment. - Key recovery using CPA analysis of a leaky reference implementation of AES-256 for setup validation. - Transfer of Technology, SCA Lab Setup at C-DOT, New Delhi and Hands-on training
2	**Technology Area**	Telecom Network and Cybersecurity
3	**Project Introduction**	Side-channel analysis (SCA) is a method of exploiting unintentional information leakage from a process in a device. The central idea of side-channel analysis is to compare some secret data-dependent predictions of the physical leakages and the actual (measured) leakage to identify the data most likely to have been processed. Side-channel analysis consists of two steps, commonly referred to as identification and exploitation. The identification consists of understanding the leakage and building suitable models. The exploitation consists of using the identified leakage models to extract the secret key. In computer security, a side-channel attack is any attack based on extra information that can be gathered because of the fundamental way a computer protocol or algorithm is implemented, rather than flaws in the design of the protocol or algorithm itself (e.g., flaws found in a cryptanalysis of a cryptographic algorithm) or minor, but potentially exploitable, implementation weaknesses. Hence, even though algorithms could be mathematically secure, its implementation might leave it vulnerable to side channel analysis thus making it unsecure. Thus, SCA is an important step in the development of cryptographically secure products. C-DOT invites participation from the Indian start-ups/ organizations/ research and academic Institutions in a collaborative solution led by C-DOT for the development of Side Channel Analysis Setup using SAKURA-X. The potential participants should have domain expertise in computer and FPGA programming, Cryptography, SCA etc. The final outcome of the collaborative development project shall be a SAKURA-X based working setup with complete input control (Plain text and Key) and should capture/store Power/EM traces of AES and other crypto algorithm implementation with corresponding plaintext in an aligned manner for TVLA and CPA analysis. Through a process of rigorous technical evaluation, C-DOT shall select participants holding the most promise of delivering commercial grade outcomes as its development partners (“Partner”) in the project. In order to achieve an efficient, accurate and production-ready solution, C-DOT would prefer to select multiple Partners for the same work item wherever feasible.

4	**Description**	The main objective of the project is to develop a methodology for capturing side channel data leakages through real-time Power Usage Change and Electromagnetic emissions (EM) emitted from an FPGA while running a cryptographic algorithm implementation on it. The side channel leakage capturing hardware framework is to be based on SAKURA-X COTS SCA reference board and an Oscilloscope. SAKURA-X (Side-channel AttacK User Reference Architecture) is a commercially available reference board specifically designed by AIST, Japan for performing Side Channel Leakage assessments of crypto HDL implementations. SAKURA-X has two on-board FPGAs. One is Controller FPGA (Spartan-6) for Input/output data handling and the other Crypto FPGA (Kintex-7) is for running the crypto algorithm implementation under test. An internal on-board interface exists between Controller and Crypto FPGA for configuring the under-test crypto algorithm implementation. As an example, for AES-256 FPGA implementation differential power leakage assessment using above hardware framework setup, the HDL implementation bitstream is programmed in SAKURA-X Crypto FPGA using JTAG interface. A pair of Plain Text and Random Key is fed to Crypto FPGA through Control FPGA I/O and the AES-256 algorithm ciphertext output is then received back through the same control FPGA I/O interface. The received ciphertext from Crypto FPGA for a given pair of plaintext and random key is saved on a PC. Suitable trigger conditions are embedded into AES-256 HDL implementation, which when fulfilled, toggle an output GPIO pin of SAKURA-X. This GPIO is connected to an oscilloscope input and based on this trigger, it starts recording power traces being fed to it from SAKURA-X Input Power Tap point (SMA port) through a SMA-BNC low noise cable. Based on above framework requirement, following modules are required to be designed and implemented for: - **SAKURA-X Controller FPGA (Spartan-6 XC6LX45-2FGG484C)** The control FPGA acts as an interface between an external PC and Crypto FPGA. A USB interface is provided on-board SAKURA-X for I/O purpose. Verilog based IP core implementation is required for following subsystems: - • Serial Communication Controller (USB/UART) for data exchange with PC (plain text, random keys, cipher text) • Input/Output (I/O) data controller (Plain text, Cipher text, Keys) for interacting with Crypto FPGA and an external PC. • Clock controller **SAKURA-X Cryptographic FPGA (Kintex-7 XC7K160T-1FBGC)** The cryptographic FPGA is where any crypto implementation under test is run based on inputs and configuration received from Controller FPGA. Verilog based IP core implementation is required for following subsystems: - • A Reference implementation of AES-256 (any mode) with embedded trigger and trigger mapping to SAKURA-X GPIO pin

		• Interface specification for inserting any other AES/Crypto implementation from a third-party or C-DOT. It includes integration of C-DOT provided AES-256 GCM implementation with the test framework. **External PC (Windows 11)** The task of external PC is to generate plain text and random keys and to receive ciphertext from SAKURA-X. Following modules are required for PC • Input/Output (I/O) control software module. This will control feeding of plain text and random keys to SAKURA-X Serial interface (USB/UART) and shall receive the generated cipher text for the given input from SAKURA-X on the same interface. It shall also interact with a Windows 10/11 based oscilloscope for performing remote operations on it. This module can be designed using general purpose programming language such as Python, C, C#, C++, MATLAB etc. It is also expected to save plain text along with captured traces in an aligned manner. **Oscilloscope** The oscilloscope shall be used for capturing the side channel leakage traces based on certain trigger events from SAKURA-X board. It shall also interact with external PC based I/O control software module over Ethernet for any remote procedure call and transfer of captured traces. Power/EM traces should be saved with the respective Plain text. This is required for Correlation Power Analysis (CPA) type attack analysis. • Windows based Oscilloscope: The Oscilloscope available with C-DOT is a Teledyne-LeCroy Mixed Digital Signal Oscilloscope (WavePro 404HD-MS, 12 Bit ADC, 4 Ch, 1000 Mpt/Ch Analog, 32GB RAM, 20GS/s, 4Ghz Bandwidth, Windows 10, Teledyne-LeCroy MAUI™ with OneTouch, Intel® Core i5-6500, 2 Ethernet RJ-45, 4 USB 3.0, 1 HDMI, 512 GB Internal Hard Driver). The oscilloscope has various connectivity options over ethernet (using VICP or LXI), USB. • It is expected that delivered side channel analysis setup framework will integrate the above mentioned oscilloscope. The same has to be validated in the C-DoT lab during integration of the side channel analysis system. **Clock and Trace Synchronization** As every hardware unit and interface is working on different clock cycles, it is pertinent that proper synchronization is established between disparate clock domains so that no data loss or misalignment occur while traces are being captured. Following framework is required to be designed for fulfilling above essential requirement • Configuration of internal clocks and synchronization between external and internal clocks for error-free data transfer. • Synchronization among external PC, Controller FPGA, Crypto FPGA modules and oscilloscope to capture noise-free and aligned side channel leakage traces with respect to input plain text and random keys. A brief sample diagrammatic representation of the hardware setup for power leakages capture for AES is given below (arrows denotes connections):



SCA Lab Setup at C-DOT New Delhi and Transfer of Technology

C-DOT is in a process of developing a dedicated Side Channel Analysis (SCA) lab setup in its New Delhi premises. It shall be used for SCA testing of HDL (FPGA) implementation of standard and proprietary cryptographic algorithms. As a first setup, the SAKURA-X based framework shall be used for performing leakages (Power/EM) capture for Correlation Power Analysis (CPA) and TVLA type analysis. In this regard, following activities needs to be performed by partner: -

- Transfer of technology (ToT): Complete transfer of all source code along with proper documentation. This will include complete code walkthrough and hands-on training to C-DOT staff members.

- Hardware Setup in Lab: Test framework setup in C-DOT, New Delhi lab and integration with C-DOT provided Oscilloscope and SAKURA-X board.

- Reference Implementation: A reference leaky implementation of AES-256 (any mode) with embedded triggers at specific points shall be provided and CPA analysis performed using traces captured on C-DOT's WavePro 404HD-MS oscilloscope and with golden test vectors shall be demonstrated for validation of work. Inspection Report from C-DOT shall be based on successful CPA demonstration by the partner in C-DOT lab and ToT completion.

5	**Roles & Responsibilities of C-DOT**	C-DOT provide technical development assistance, infrastructure and financial support to the project partners selected through a process of evaluation and due diligence conducted by a committee of subject experts. Wherever deemed necessary, C-DOT may arrange resources, equipment, training, testing infrastructure, mandatory clearances, statutory permissions, and provide gap funding to the partners in realizing the respective target deliverables. Development costs of the module, whether developed from scratch or derived from existing background technology of partners shall be borne by C-DOT. C-DOT shall use the final solution for integration with production grade software and SCA lab setup. C-DOT reserves the right to modify and enhance the solution and provide it to C-DOT customers or other Partners. C-DOT shall engage with Partners on a non-exclusive basis and shall retain its right to develop similar products / through other developmental programs. C-DOT Delhl GST No: 07AAATC3895K1ZD
6	**Roles & Responsibilities of Participants**	The Partner(s) may build the required module afresh or by modifying pre-existing background technologies available with them. The Partner(s) may utilize the available test and infrastructure facilities offered by C-DOT with no financial implication for its usage. All commercial proposals shall include manpower and other costs breakup (Capital, Consumables, Travel, DA, Training, Contingency, Overhead, GST etc.). Participation in the project shall be on a non-exclusive basis. All partner(s) shall be required to demonstrate commitment to the project by entering into a formal agreement with C-DOT as per the CCRP policy.
7	**Expected Deliverables**	• PC (Windows) application module: Input/Output Control Software module written in a suitable language (Python, C, C#, MATLAB etc.). For a better idea as to what degree I/O control is required, Rambus TVLA with AES document (see resources) can be referred. • PC (Windows) application module: Input/Output Control Software module for remote-procedure based control of Oscilloscope in order to obtain power/EM traces aligned with input plaintext and the associated ciphertext. Power/EM traces can be stored remotely on a computer or on the oscilloscope itself. • Power/EM traces are to be saved with the respective Plain text. This is required for Correlation Power Analysis (CPA) type attack analysis. Remote Procedure calls of WavePro 404HD-MS Oscilloscope are to be used in I/O Control Software to achieve this alignment. • IP cores for SAKURA-X Control FPGA for interfacing with PC I/O Control software module and Crypto FPGA for transfer of plaintext, keys, ciphertext across different clock domains. AIST provided HDL files can also be used after suitable modification. • Synchronization between external PC, Controller FPGA, Crypto FPGA modules and oscilloscope for aligned capture and recording of noise-free side channel leakage traces with respect to input plain text and random keys. • A leaky reference implementation of AES-256 (any mode) with embedded triggers at specific points of the algorithm. Key recovery using CPA analysis is required to be demonstrated for qualifying the solution as a usable setup.

		• Software setup Integration with C-DOT provided AES 256 GCM IP Core. AES module Interface details (with trigger pin details) to be provided to C-DOT team at-least 1.5 month before project completion for wrapper generation. C-DOT will endeavor to provide AES IP Core with required interfaces within 10 working days. • Software and IP core installation, testing and commissioning on C-DOT owned equipment (SAKURA-X, Windows 11 PC, Teledyne-Lecroy WavePro 404HD-MS Oscilloscope, Cable and probe for Power and EM trace capture) in C-DOT Delhi SCA Lab. • Transfer of technology (ToT) (Design, Software and HDL code walkthrough, IP core resynthesis, HDL test bench, Setup development, Synchronization scheme, Detailed design documentation, Test plan and report), 10 working days hands-on training and Power/EM trace capture demonstration to staff members on SCA lab setup established in C-DOT New Delhi premises. • A development setup for enhancement of provided solution shall be established by the partner in C-DOT Delhi SCA Lab. C-DOT shall provide suitable software licenses for this purpose in SCA Lab PCs, if not already procured by the partners from the project funds. • Provided HDL source code should be synthesizable using AMD-Xilinx Vivado 2019.1 development suite or higher version. • Installation, integration and commissioning of setup in C-DOT Delhi SCA lab – 10 working days. This shall be exclusive of ToT activities period. • Bug-fixing, onsite support (C-DOT Delhi) and enhancement required, if any – till 1 year after initial delivery and acceptance. • Total duration of project is around 6 months max. In exceptional circumstances, any extension shall be based on a mutual agreement and availability of funds. • All specialized equipment such as reference boards, PCs, cables etc., capital items, software licenses purchased for this project by the partners from the approved funds shall be transferred to C-DOT and re-established in C-DOT Delhi SCA Lab as fully functional development setup. • Partners to make use of Windows based Lecroy Oscilloscope (WavePro 404HD-MS) available with C-DOT for trace capture in C-DOT Delhi SCA lab. For development purpose at partner's site, new oscilloscope may not be procured from project funds and a similar one can be taken on rent/loan through iSTEM by the partners, if required. It shall be returned to iSTEM agency after project completion as per iSTEM's T&C. • Deliverables approval is subject to a successful internal evaluation by C-DOT and assistance is to be provided during inspection phase, as and when necessary. • Project monitoring shall be done by a committee constituted as per C-DOT CCRP policy guidelines.

8	**Ownership of Background & Foreground IP**	Background technologies used in the project shall continue to remain with the respective owners. New foreground technologies created during the project shall be owned by the respective development partners, individually or collectively as the case may be. Any agreement required for collective ownership shall be settled directly by the concerned partners. The ownership of the final solution shall rest collectively with C-DOT and all its partners."

Important Resources:

Oscilloscope:
https://www.teledynelecroy.com/oscilloscope/wavepro-hd-oscilloscope/wavepro-404hd-ms
SAKURA-X Documentation
https://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-X.html
http://www.risec.aist.go.jp/project/sasebo/download/SASEBO-GIII_Spec_v1_1_English.pdf
https://web.archive.org/web/20160806152144/http://www.risec.aist.go.jp/project/sasebo/download/SASEBO-GIII_QSG_English.pdf
https://www.risec.aist.go.jp/project/sasebo/download/SASEBO-GIII_QSG_English.pdf
https://www.risec.aist.go.jp/project/sasebo/

Software:
https://www.risec.aist.go.jp/project/sasebo/download/sasebo_giii_materials.zip

RamBus Document
https://www.rambus.com/wp-content/uploads/2015/08/TVLA-DTR-with-AES.pdf

Technology Areas (XXXX)

PQC	Post-Quantum Cryptography
TVLA	Test Vector Leakage Assessment
CPA	Correlation Power Analysis
DPA	Differential Power Analysis
EMA	Electromagnetic Emission Analysis
SCA	Side Channel Analysis
OTHR	Other