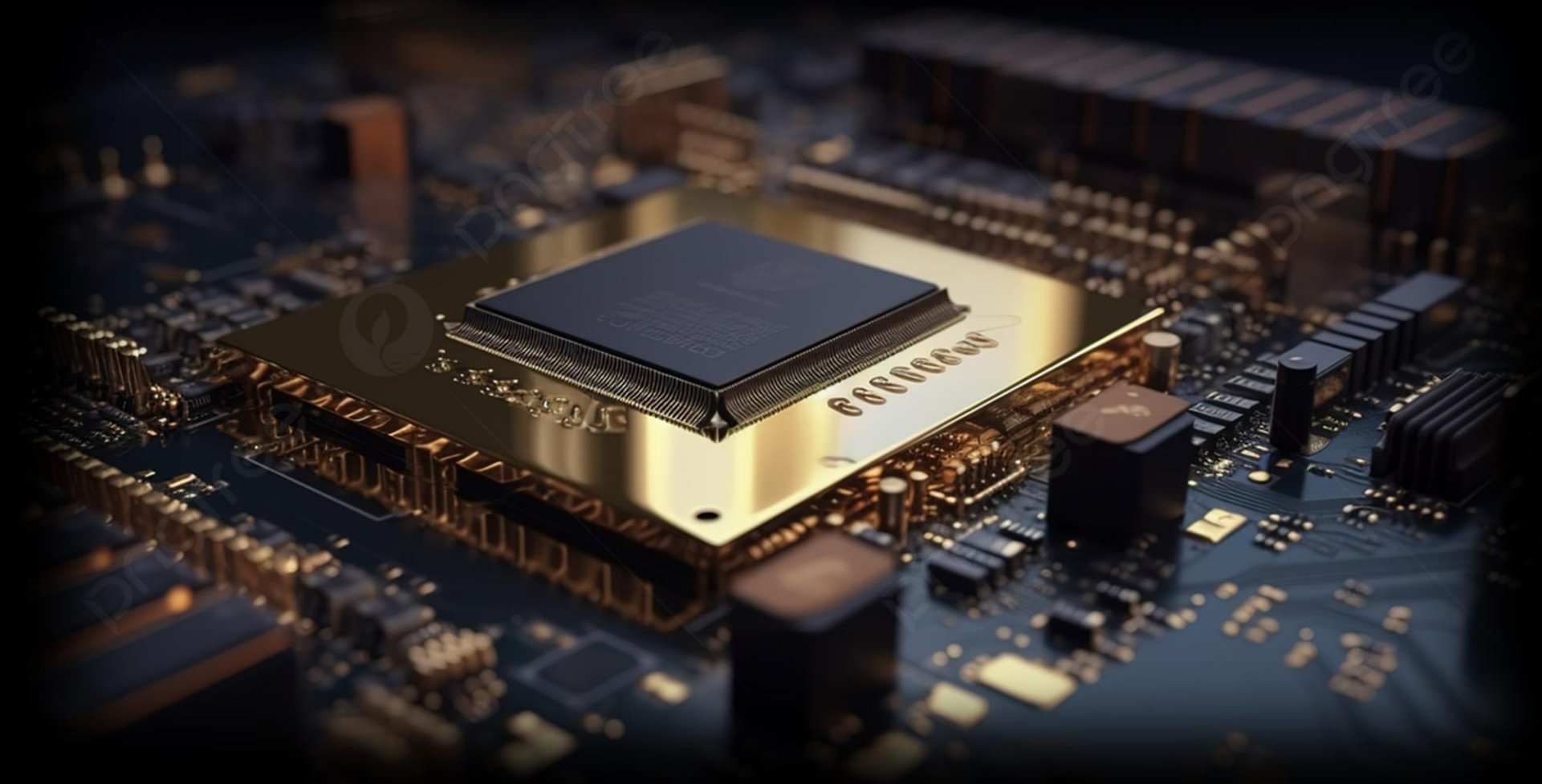


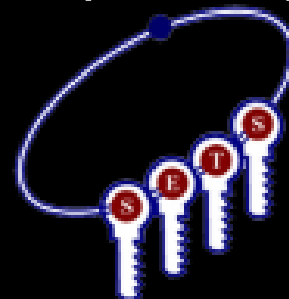


Reflections on ISO/IEC 17825: Gaps in Commercial Frameworks and the Need for Standard APIs

Renita J and Suganya Annadurai

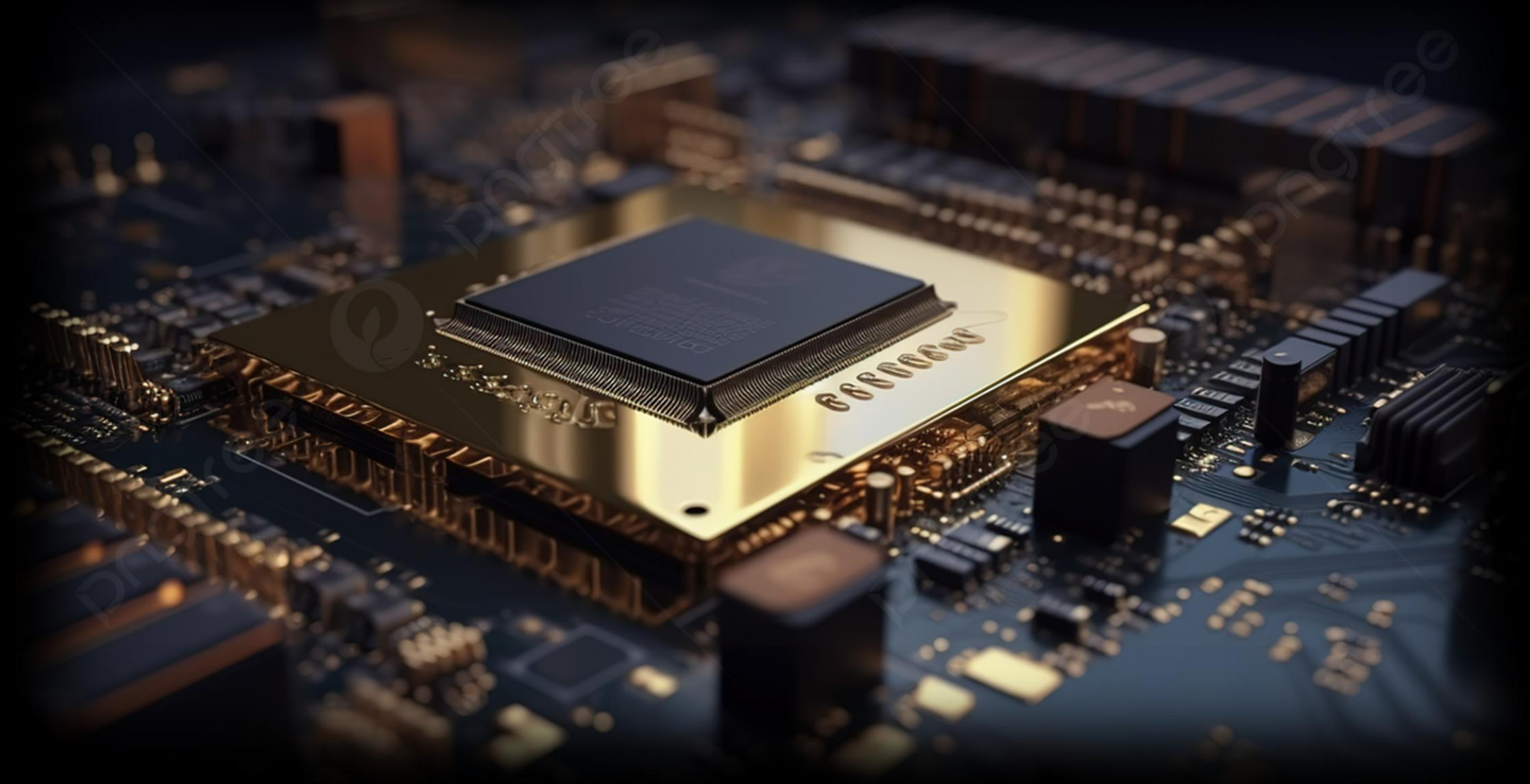
Society for Electronic Transactions and Security

(SETS)

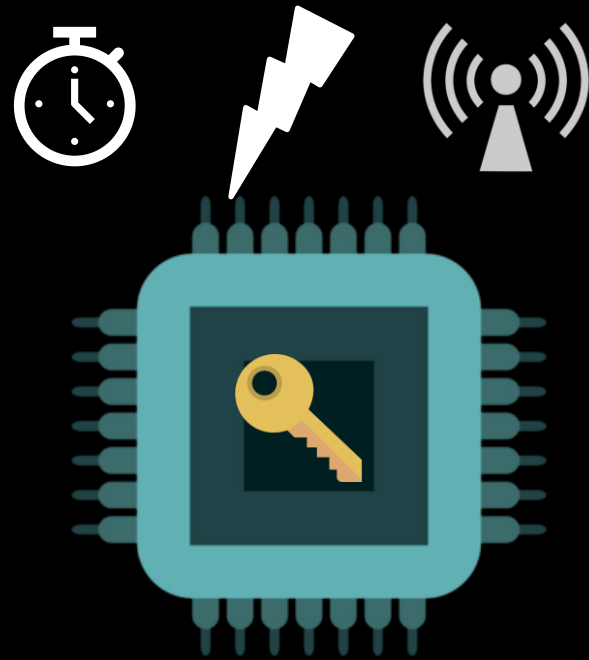


Overview

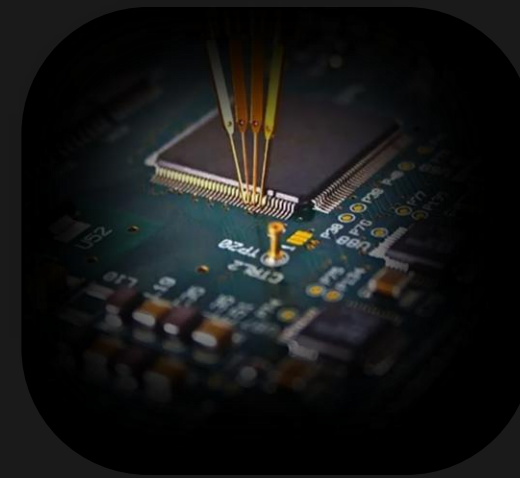
- **Introduction to ISO/IEC 17825**
- **Role of ISO/IEC 20085:1**
- **Identified Challenges**
- **Key Aspects**



Side Channel Testing



ISO/ IEC 20085



Measurement and Analysis Tools



FIPS 140-3 and ISO/IEC 19790

FIPS 140-3 (Federal Information Processing Standard) and ISO/IEC 19790 (international equivalent) define security requirements for cryptographic modules.

Both standards ensure that hardware and software implementations of cryptography meet globally recognized assurance levels

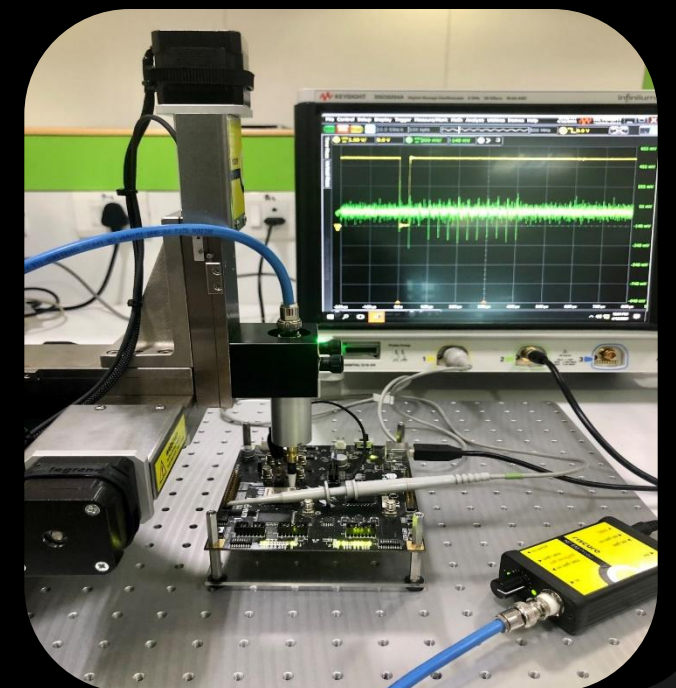
Security Level - 3

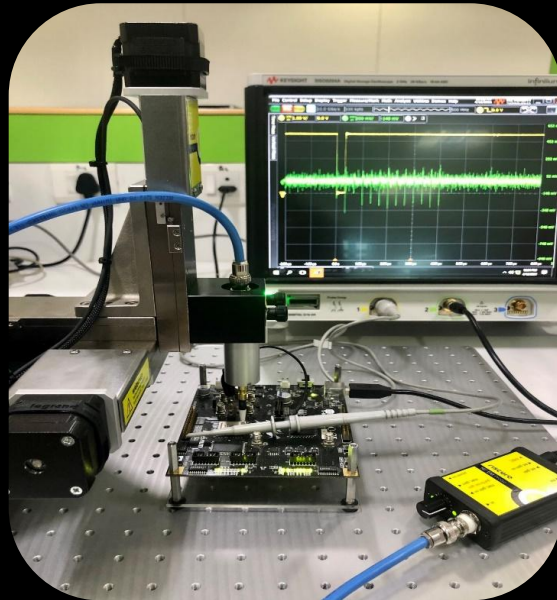
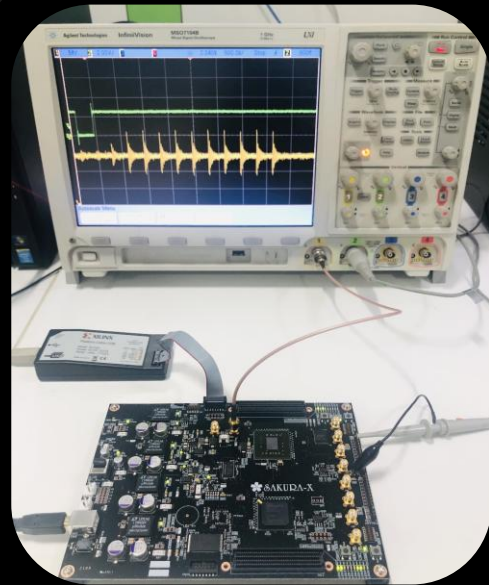
Security Level - 4



ISO/ IEC 17825

Resistance Against Physical Attacks





Power: via current probe/conductor between supply IUT.

EM: probe placement crucial; signals may be amplified.

Timing: measure difference between operation start result return.

Tools: probes, amplifiers, filters, digitizers, trace storage

Measurement

Test Methods

Timing analysis

Simple Power/EM analysis

Differential Power/EM Analysis

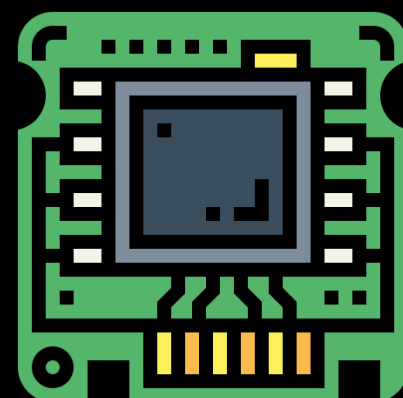
ISO/IEC 17825

ISO/IEC 20085

Defines measurement tools environment requirements.

Covers power, EM, and timing measurements.

Ensures consistent accurate evaluations with automation support



ISO/IEC 19790

Assurance

Tests confirm that design shows measured resistance against practical attacks

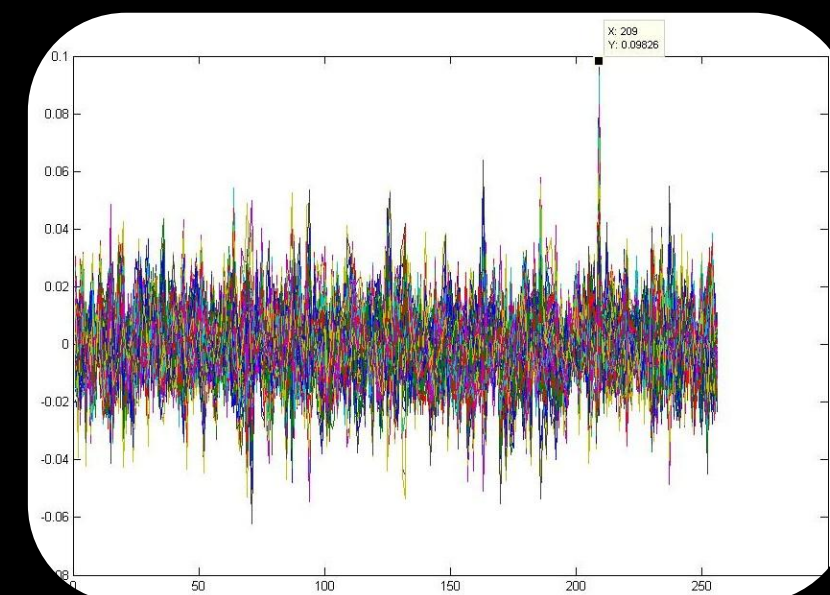
Analysis

Automate measurement trace collection.

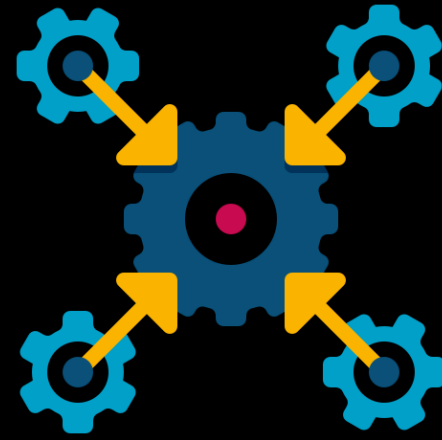
Preprocess: remove abnormal traces, align using POIs, reduce data (PCA).

Postprocess: filtering, chaining, frequency statistical analysis.

Identify potential side-channel attacks



Automation



Interoperability

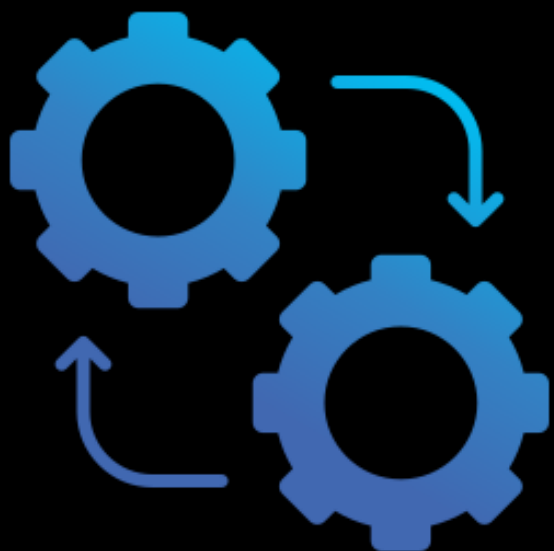


Need for Standard APIs

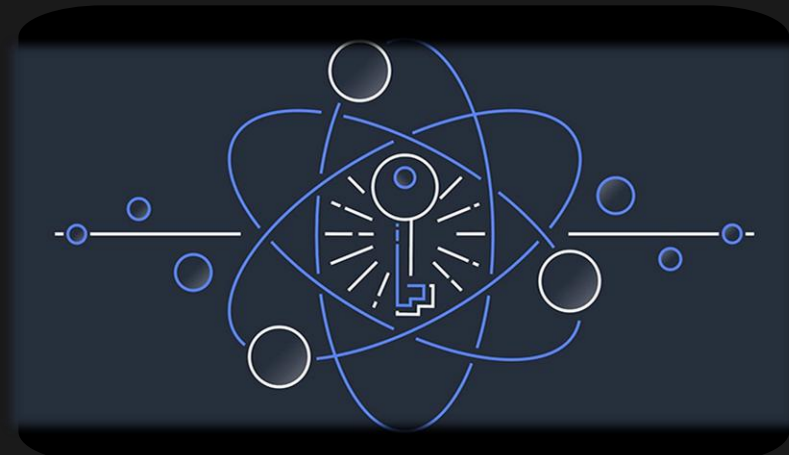
1. **Automate** ISO/IEC 17825 tests across different platforms for commercial frameworks
2. Provide **availability** of defined parameters in ISO 17825
3. Overcome **testing limitations** such as number of traces, key recovery, and partial key recovery
4. Incorporate **AI-based attacks** in the evaluation scope
5. Support testing of **post-quantum** cryptographic algorithms

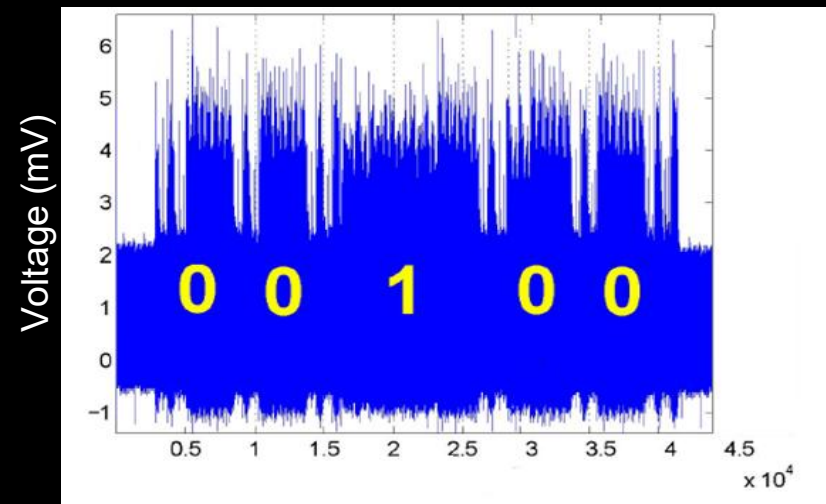


Integration

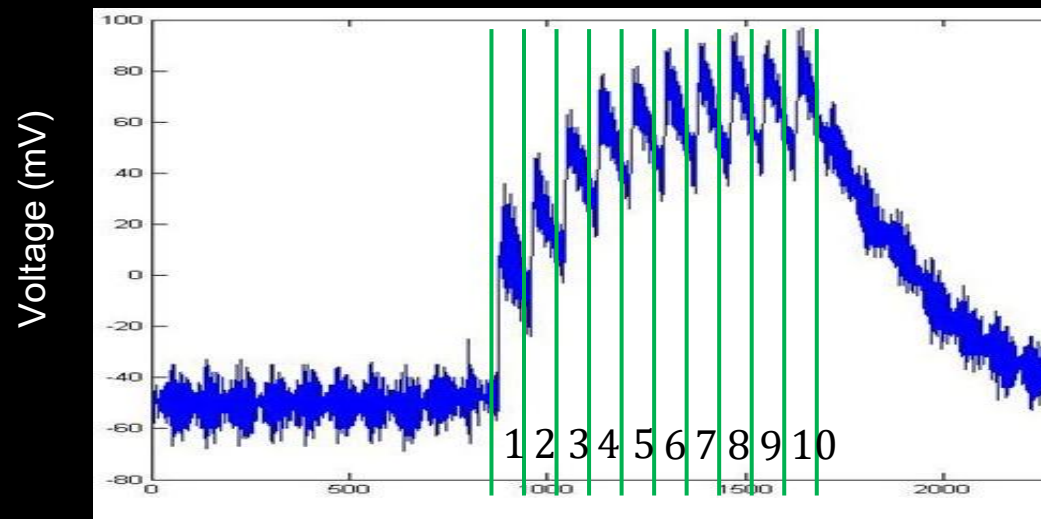


Open-Source Implementation



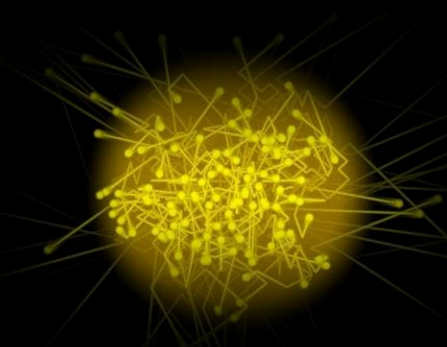


Trace points



Trace points

**Trace
Averaging**



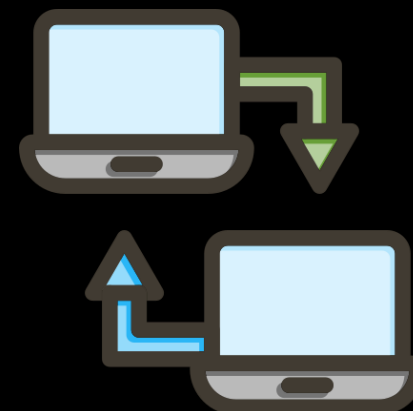
**New Side
Channel
Attacks**

Signal Quality



Key Aspects

Data Portability

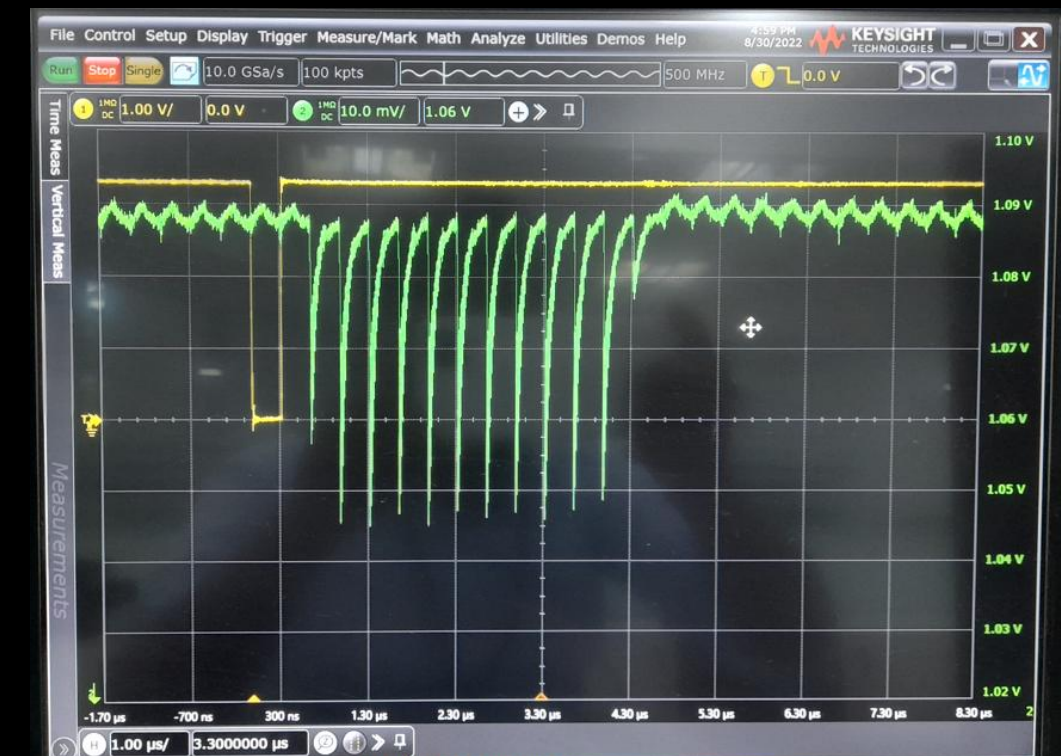


Calibration

ISO/IEC 20085:2



Adaptability



Thank You

asuganya@setsindia.net

renita@setsindia.net

