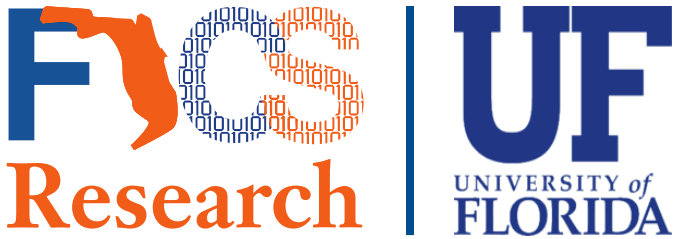
TDM: Time and Distance Metric for Quantifying Information Leakage Vulnerabilities in SoCs

Avinash Ayalasomayajula, Henian Li, Hasan Al Shaikh,
Sujan Kumar Saha, and Farimah Farahmandi



Outline

- Background and Motivation
- Threat Model
- Security Asset protection
- Asset Flow Graph
- Time and Distance Metric definition
- Proposed Workflow of TDM framework
- Experimentation
- Result Analysis
- Conclusion

Background and Motivation

Background:

- Heterogeneous System-on-Chips with numerous IPs increase complexity that leads to security vulnerabilities.
- Information leakage where sensitive data are compromised is one of the crucial security vulnerabilities in hardware designs.
- Information leakage can occur due to design flaw, tool-based design optimization, or malicious actions.
- Very few research have been done on properly quantifying the information leakage vulnerability in hardware domain.

Motivation:

- Quantifying Information leakage vulnerability with appropriate metric will help designers to decide on the priority of applying countermeasures.
- Existing Graph-based models [2,3], corruptibility and confidentiality [4], and min-entropy leakage [5] do not consider dynamic interaction of assets both in spatial and temporal dimensions.
- This work proposes information flow tracking based Time and distance metric for information leakage assessment.

Threat Model

Primary Concern: Information Leakage

- Adversaries with access to design input/output ports may exploit the design for unauthorized data access.
- The risk of potential data leaks from internal registers by adversaries.

Adversaries' Techniques

- Potential use of sophisticated attack methods to extract information from the internal registers.
- These attackers are skilled enough to perform various attacks such as fault injection, side channel etc. to extract device secrets.

Objective

- To focus on developing a set of design metrics that assess hardware designs and provide a quantitative measure of the risk associated with information leakage.

Scope of Analysis

- Focus on design metrics in the context of possible information leakage
- While recognizing attack vectors like fault injections, side channel etc. an in-depth analysis of these attack methods is beyond this task's functional scope.

SoC Security and Asset Protection

SoC Security and Asset Protection

- Protecting security assets is crucial for overall SoC integrity.
- Trace and map all design signals/registers affected by asset flow.
- Identify and secure registers with complete or partial exposure to security asset flow. We name these secondary assets.

Complete Flow Registers: Registers that capture the entire security asset data without alteration through the design's signal paths. Any data leaks from these registers can provide the adversary with access to the device secret.

Partial Flow Registers* : Registers that capture data derived from security assets after it has been processed or altered by combinational logic, resulting in only a portion of the original data being propagated through to these registers.

Asset Flow Graph

Identification of Primary Security Assets

- Define critical elements such as primary inputs and internal registers using design specifications, previous security incidents, and vulnerability databases.

Asset Flow Graph (AFG) Creation:

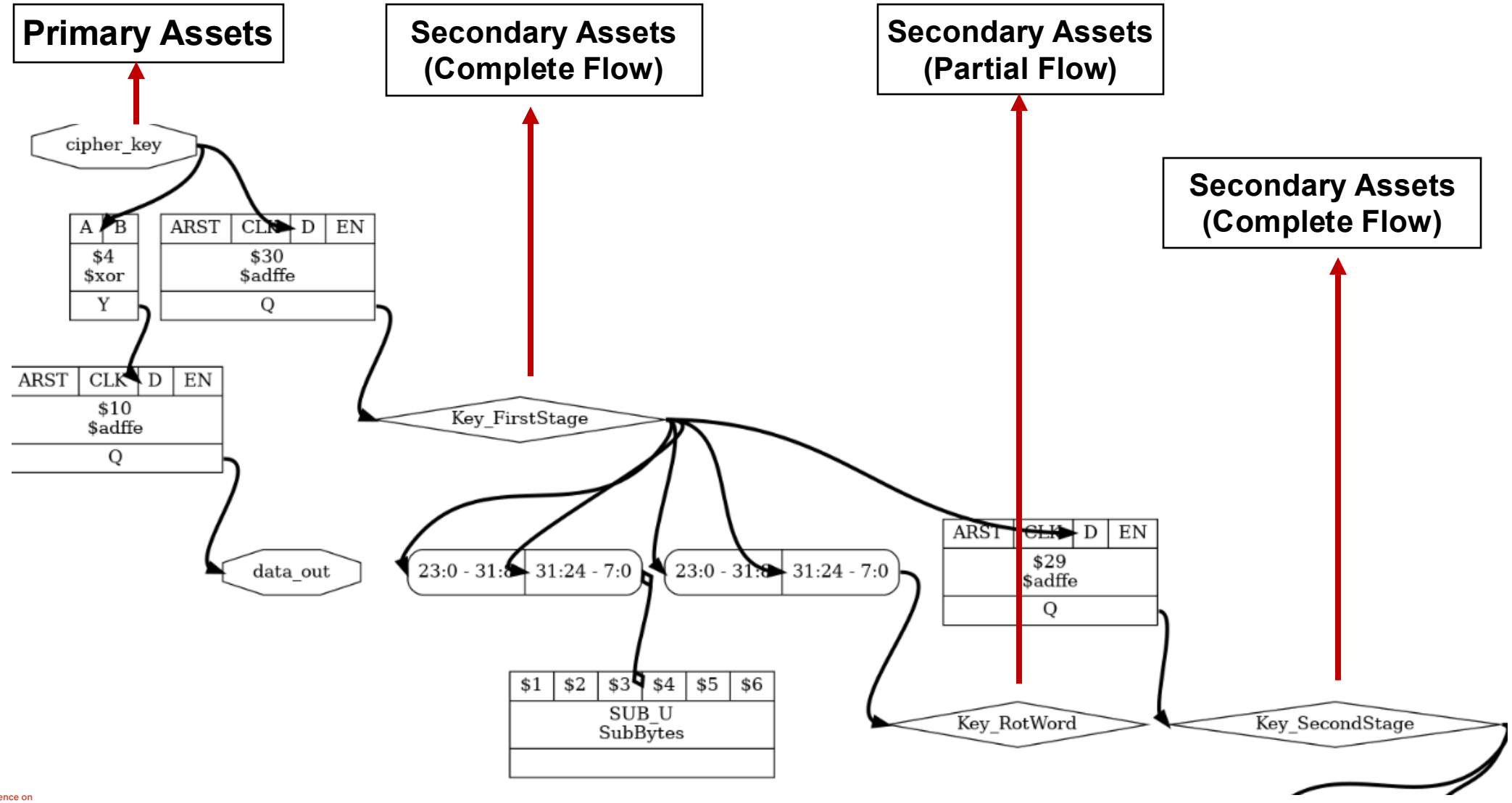
- Perform static analysis using ‘Yosys' for generating an Abstract Syntax Tree (AST) from RTL design files.
- Prunes the AST to focus on security asset pathways, forming the AFG.
- AFG illustrates detailed routing of security assets through SoC circuits.

Functionality of AFG:

- Represents security assets as nodes within the graph.
- Uses edges to show asset flow through combinatorial and sequential circuit elements.
- Identify secondary assets (complete, partial flow registers).

Security Assets = Primary Assets + Secondary Assets.

AFG Example : AES



Security Metrics Introduced

Introduction to two critical metrics for security evaluation: Time-based and Distance-based metrics.

Time-Based Security Metrics

- Time-based metric revolves around the operational period of security assets within the SoC.
- It assesses the risk based on how long these assets are stored and potentially exposed.
- The longer an asset is active in the hardware, the greater the window for adversaries to execute attacks.
- This metric includes analyzing the time window for attack execution and the duration of information exposure.

Distance-Based Security Metrics

- Focuses on the physical layout of security-critical signals/registers relative to output ports.
- The proximity of these elements to observable points is crucial for assessing leakage risks.
- Threats vary based on whether critical registers are too close to or too far from output ports.
- The metric defines 'distance' as the number of register stages from a register to the output, influencing the vulnerability to information leakage.

TD Metric Definitions

- **Time Metric, T(A, R, N):** The maximum number of clock cycles where security asset **A** remains unchanged in register **R** starting from clock cycle **N**.

- **Distance Metric, D(A, R, O):** The number of register stages data must traverse from design register **R** to output port **O**, where security asset **A** propagates.

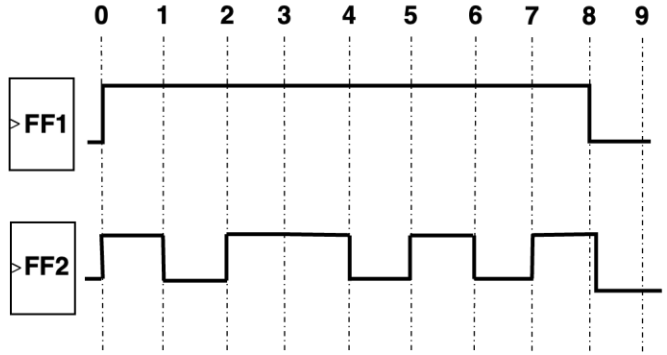
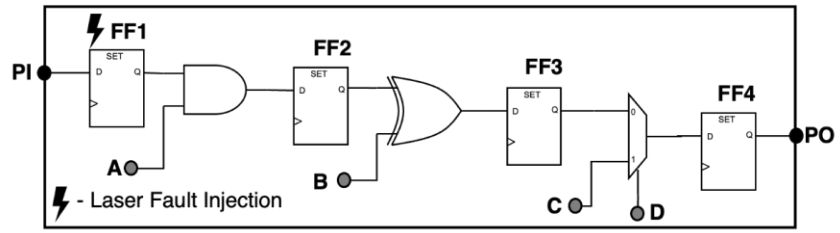
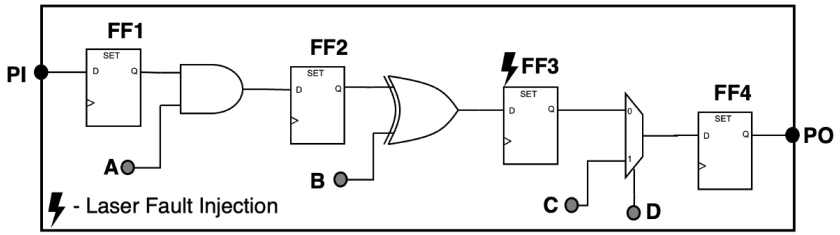


Figure 1: Time metric illustration for FF1 and FF2



(a)



(b)

Figure 2: Distance metric illustration with FF and logic gate showing fault propagation from FF1 (a) and FF3 (b)

Proposed Workflow of TDM Framework

- Our framework takes RTL design files and design specifications as input to the workflow.
- Primary security assets are identified from the specification.
- RTL designs are converted to Abstract Syntax Tree and using security asset tracking, Asset flow graph is generated from which secondary asset list is determined.
- Using list of assertions, formal verification is used to find time metric values of secondary assets.
- Using Fan-out analysis, distance metric values are determined.

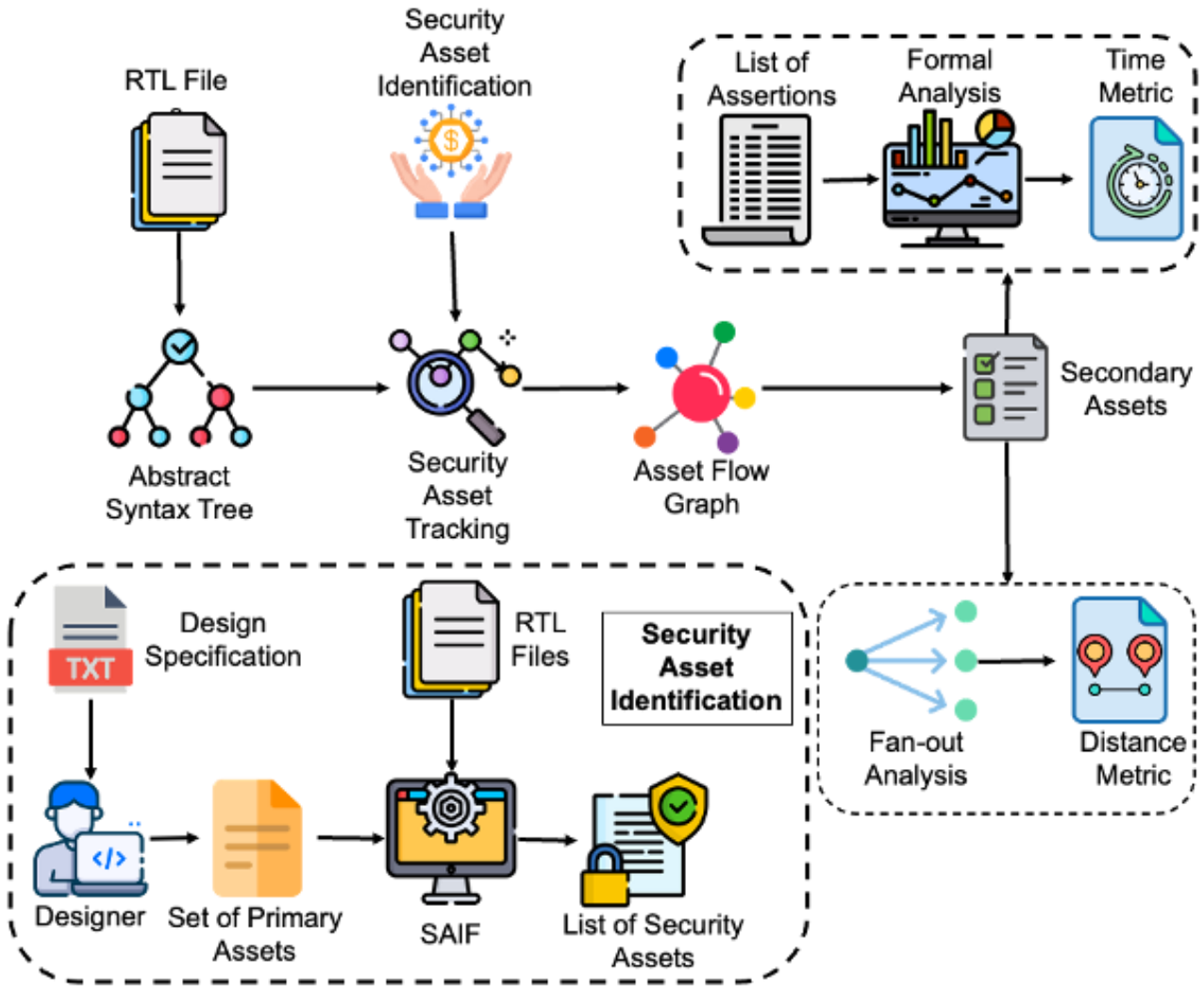


Figure 3: Information leakage assessment workflow

Experimentation

- We perform our analysis on three versions of AES, SHA256, and HMAC hardware IPs.
- The security properties related to assets are developed and formal analysis is performed.
- Considering fault injection as potential attack, we perform transient fault analysis on the IP benchmarks and analyzing 143,808 faults using Synopsys Z01X tool.
- The following are some properties of AES designs considered for this experimentation.

SP 1: $M_{3,0}^{9}$of AES should not be faulty at the 9th round's cycle(s).

SP 2: $K_{i,0}^{9}$, $(i \in \{0,1,2,3\})$ of AES should not be faulty at the 9th round's cycle(s).

SP 3: M^{10} of AES should not be faulty at the 10th round's cycle(s).

SP 4: M^{9} of AES should not be faulty at the 9th round's cycle(s).

SP 5: K^{9} of AES should not be faulty at the 9th round's cycle(s).

SP 6: $M^{10}$of AES should not be equal to any byte of K^{0}at the 10th round's cycle(s).

Result Analysis

TABLE I: Results of Time and Distance metrics for Open-source Hardware Designs

Benchmark	# of Cock Cycles	Primary Asset	# of Secondary Asset	Time Metric	Value	Distance Metric	Value
AES I	21	Key	50	Key 0	20	A10.out_1	2
AES II	12	Key	72	u0.w	1	u0.w	1
AES III	12	Key	50	RKGEN_U0.Key_FirstStage	11	U_KEY.data_out	1
SHA 256	65	Block	40	w_mem_inst.{w_mem, w_0, w_1, w_9, w_14, w}	17	w_mem_inst.{w_mem, w_0, w_1, w_9, w_14, w}	7
HMAC	140	Key	46	Key block, inner pad, outer pad	139	Sha256.w_mem_inst.{w_mem, w_0, w_1, w_9, w_14, w}	9

Result Analysis

- We identify threat level of each asset as number of security property violations.
- Risk level is determined based on threat level and time and distance metric values. The risk level is proportional to time metric value and inversely proportional to distance metric.

$$\boldsymbol{Time - oriented\ Assets\ Risk\ Level} = Threat\ level \times Time\ Metric$$

$$\boldsymbol{Distance - oriented\ Assets\ Risk\ Level} = Threat\ level \div Distance\ Metric$$

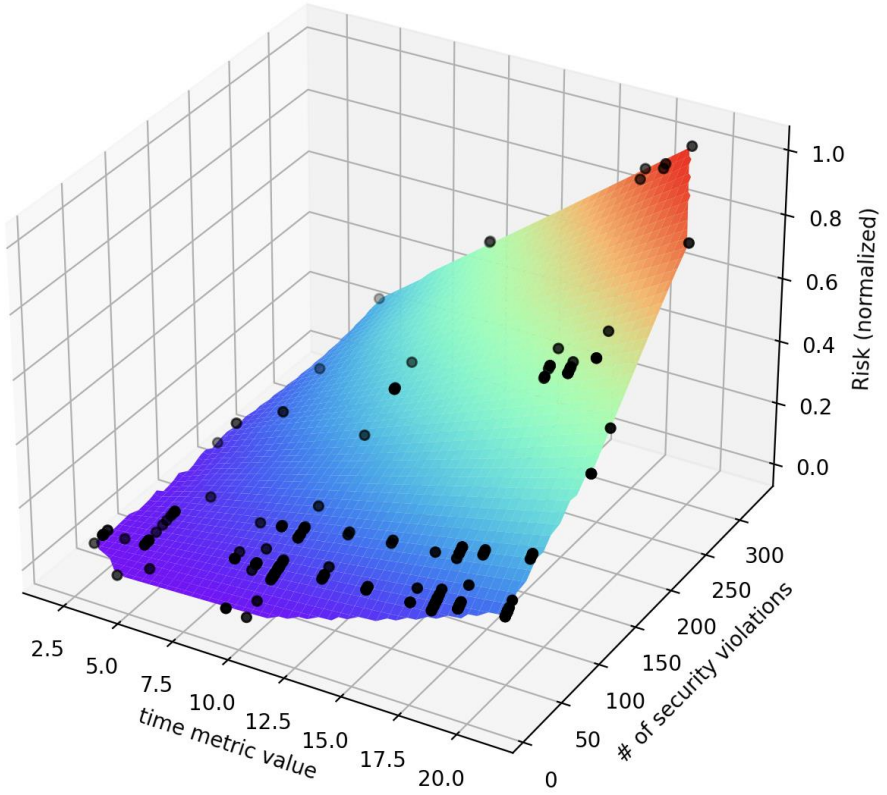
TABLE II: Top 5 Time-oriented critical assets ranked on Risk level

Asset Name	Threat Level	Attack Window	Time Metric	Risk Level
a1.out_1	212	Cycle 12→14	19	0.0777
a5.out_1	196	Cycle 20→22	18	0.0681
a2.out_1	207	Cycle 14→16	17	0.0679
a3.out_1	194	Cycle 16→18	17	0.0636
k0	153	Cycle 11→12	21	0.0620

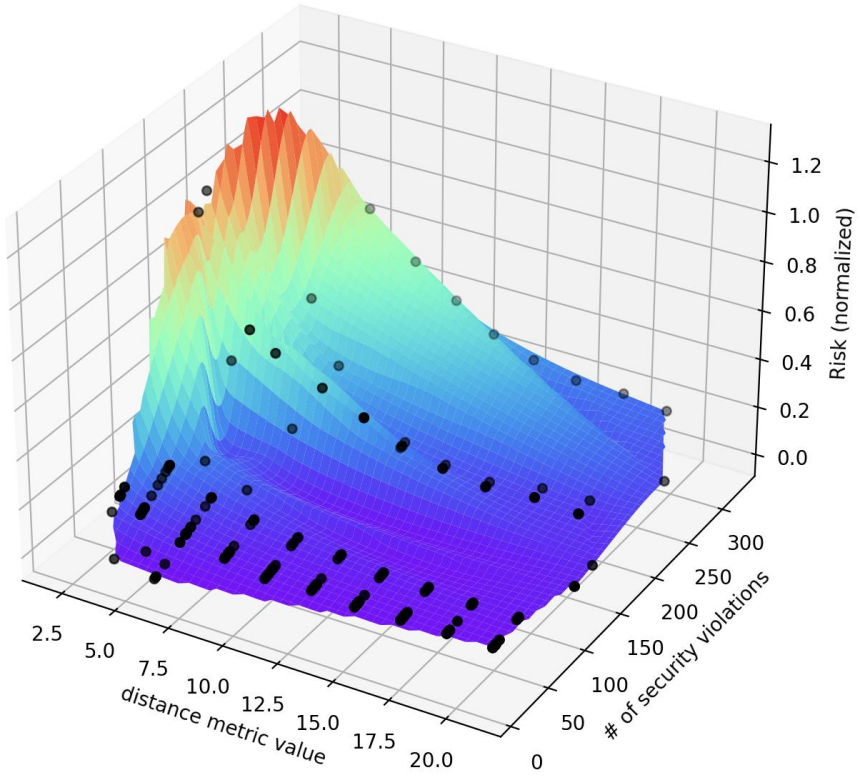
TABLE III: Top 5 Distance-oriented critical assets ranked on Risk level

Asset Name	Threat Level	Attack Window	Distance Metric	Risk Level
a10.out_1	178	Cycle 20→21	2	0.1515
a8.out_1	241	Cycle 16→18	5	0.0820
a9.out_1	163	Cycle 18→19	4	0.0693
a7.out_1	221	Cycle 14→26	7	0.0537
a6.out_1	198	Cycle 12→14	9	0.0374

Result Analysis



(a)



(b)

Figure 4: Normalized Risk Levels across 6 AES-128 Security Properties based on (a) Time Metric, and (b) Distance Metric

Conclusion

- Analyzing Information leakage vulnerability is critical in secure SoC design step.
- TDM provides a systematic way of analyzing Risk level of security assets taking their spatial and temporal proximity in the hardware.
- Experimentation is performed on multiple security IP benchmarks.
- Time- and distance-oriented risk level values provide quantitative data that guide designers in identifying the necessary countermeasures to implement.

References

[1] Somoye, I. O., Plusquellic, J., Mannos, T. J., & Dziki, B. (2024). An Engineered Minimal-Set Stimulus for Periodic Information Leakage Fault Detection on a RISC-V Microprocessor. Cryptography, 8(2), 16.

[2] Saha, S. K., Mbongue, J. M., & Bobda, C. (2022, June). Metrics for Assessing Security of System-on-Chip. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 113-116). IEEE.

[3] Meza, A., & Kastner, R. (2023). Information Flow Coverage Metrics for Hardware Security Verification. *arXiv preprint arXiv:2304.08263*.

[4] Purdy, R., Duvalsaint, D., & Blanton, R. S. (2022, June). Secuirty Metrics for Logic Circuits. In *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 53-56). IEEE.

[5] Feldtkeller, J., Güneysu, T., & Schaumont, P. (2023, December). Quantitative Fault Injection Analysis. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 302-336). Singapore: Springer Nature Singapore.

[6] Nicholas, G. S., Aklekar, D. V., Thakar, B., & Saqib, F. (2023). Secure instruction and data-level information flow tracking model for RISC-V. Cryptography, 7(4), 58.

[7] Al Shaikh, H., Monjil, M. B., Azar, K. Z., Farahmandi, F., Tehranipoor, M., & Rahman, F. (2023, October). QuardTropy: detecting and quantifying unauthorized information leakage in hardware designs using g-entropy. In 2023 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) (pp. 1-6). IEEE.

Q & A