SAND2019-8009D

The Center for Cyber Defenders

Expanding computer security knowledge

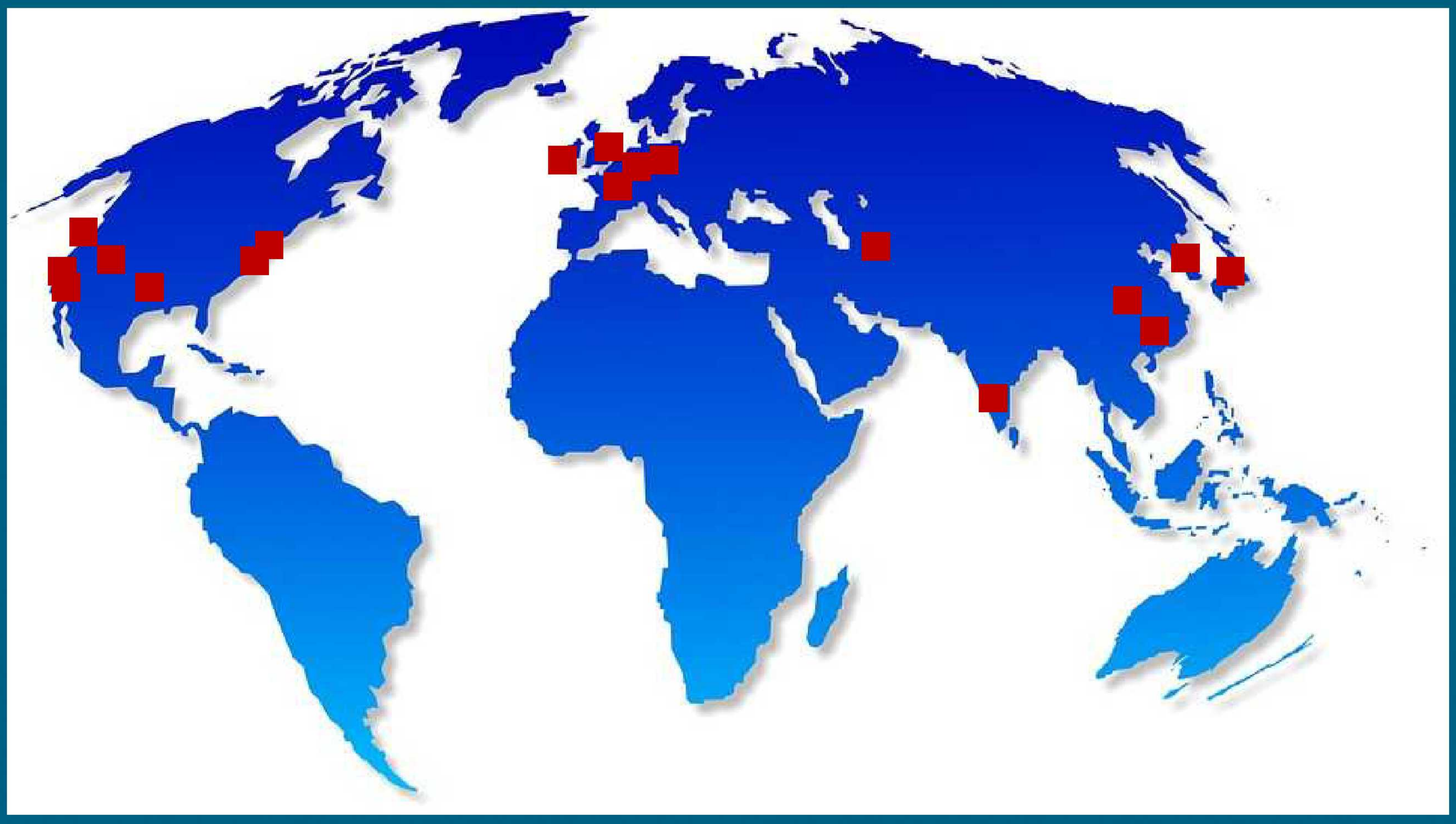
Microarchitectural Diversity

Disabling Trojans with Automated Digital Circuit Modification

Jonathan Cruz, University of Florida

Project Mentors: Jason Hamlet, Org. 5827, Vivian Kammler, Org. 5845

Problem Statement:



Global Distribution of Semiconductor IP Vendors[1]

- Untrusted third-party intellectual property (3PIP) vendors can introduce malicious functionality known as Hardware Trojans.
- It is infeasible to exhaustively test circuits to detect malicious modifications.

Objectives and Approach:

- *Goal*: Disable Trojans in digital circuits.
- Given 3PIP:
  - Convert design to graph and simulate to estimate signal probabilities.
  - Identify suspect nodes and enumerate k-bit slice.
  - Compare binary decision diagram (BDD) of k-bit slice to library of suspicious structures.
  - Merge suspect slices then diversify (add/ remove/invert) and simulate.
  - Keep changes if resulting circuit satisfies comprehensive testing.

Results

- We tested our approach on the Trojan-free and 10 Trojan-inserted variants of the XTEA benchmark mapped to IGLOO FPGA.

Benchmark	No. Gates	No. Suspect Struct.	No. Troj Struct. Identified
xtea	6138	373	0
xteaT201	6183	397	1
xteaT202	6181	412	1
xteaT203	6075	374	2
xteaT204	6147	412	4
xteaT205	6253	400	3
xteaT206	6187	368	2
xteaT207	6176	344	2
xteaT208	5916	320	1
xteaT209	6196	371	5
xteaT210	6050	405	2

Suspect Structure Identification on Trojan-Inserted designs

Impact and Benefits:

- We are able to successfully identify the Trojan structures inserted in XTEA benchmarks.
- *Next steps:* Reduce the number of suspect structures by increasing simulation effort.
- Along with standard verification techniques, diversification can be used for defense-in-depth for protecting against hardware Trojans.

[1] G. Ramamoorthy, "Market Share Analysis: Semiconductor Design Intellectual Property Worldwide, 2012", https://www.gartner.com/doc/2403015/market-share-analysis-semiconductor-design.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY NNSA National Nuclear Security Administration