Open Data-Leakage Trojan Fight-Through Capability Admits Design for Security (DFS) Techniques

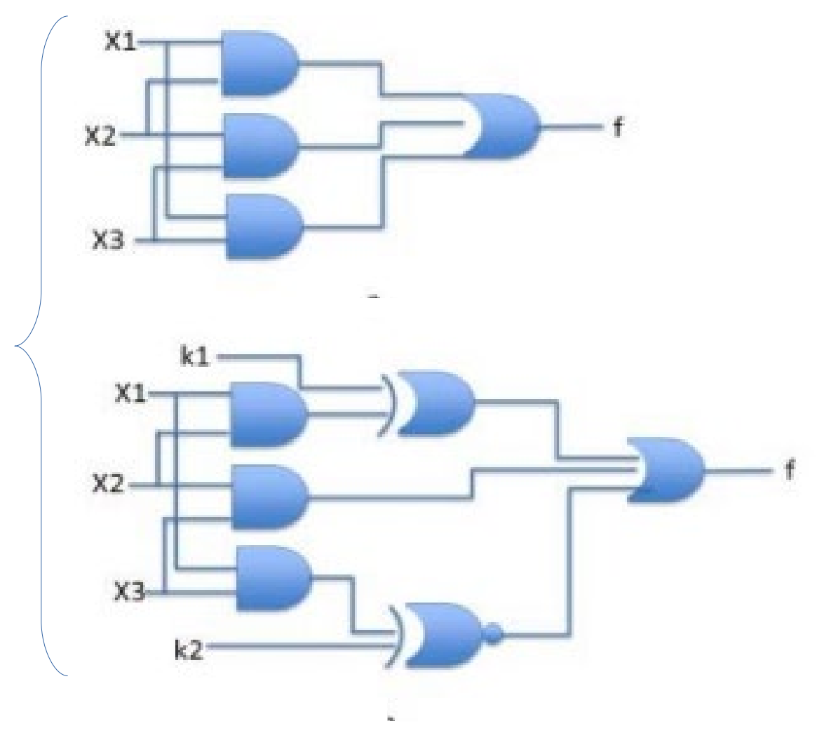
BACKGROUND:

DFS methods focus on increasing the difficulty of establishing data leakage channels by the hardware Trojan. However, they can still be compromised when the same design undergoes multiple fabrication runs, and attackers can procure a fabricated chip from one run and reverse-engineer the design. The hardware Trojans can then be designed and injected in subsequent runs.

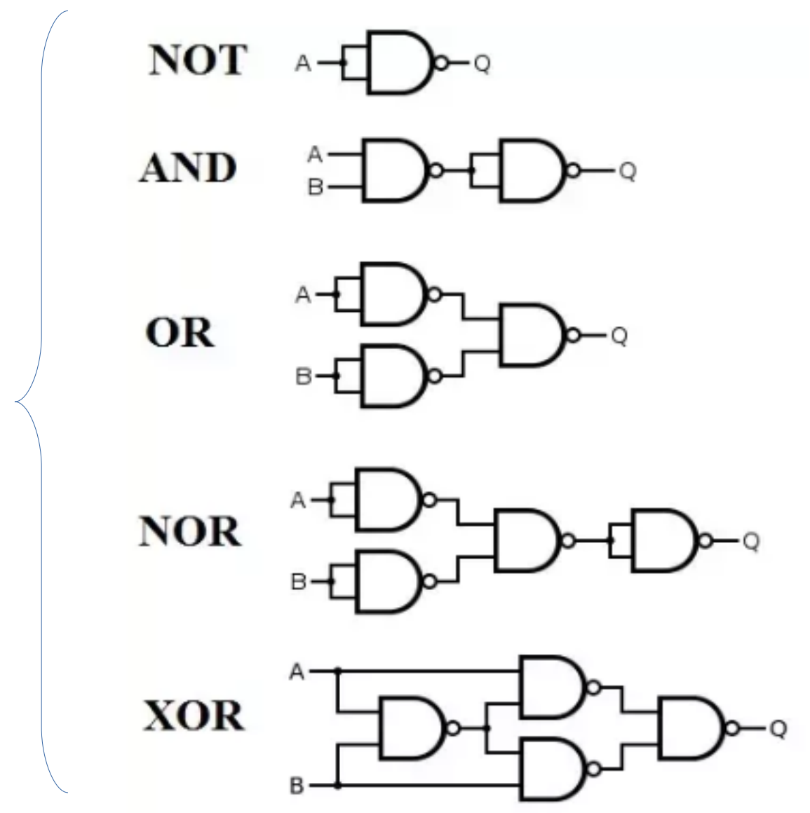
- This scenario has mostly been overlooked in the literature
- How to prevent data leakage when side channels are successful in bypassing existing DFS methods.

METHODS (3 Main Methods):

1. Obfuscation

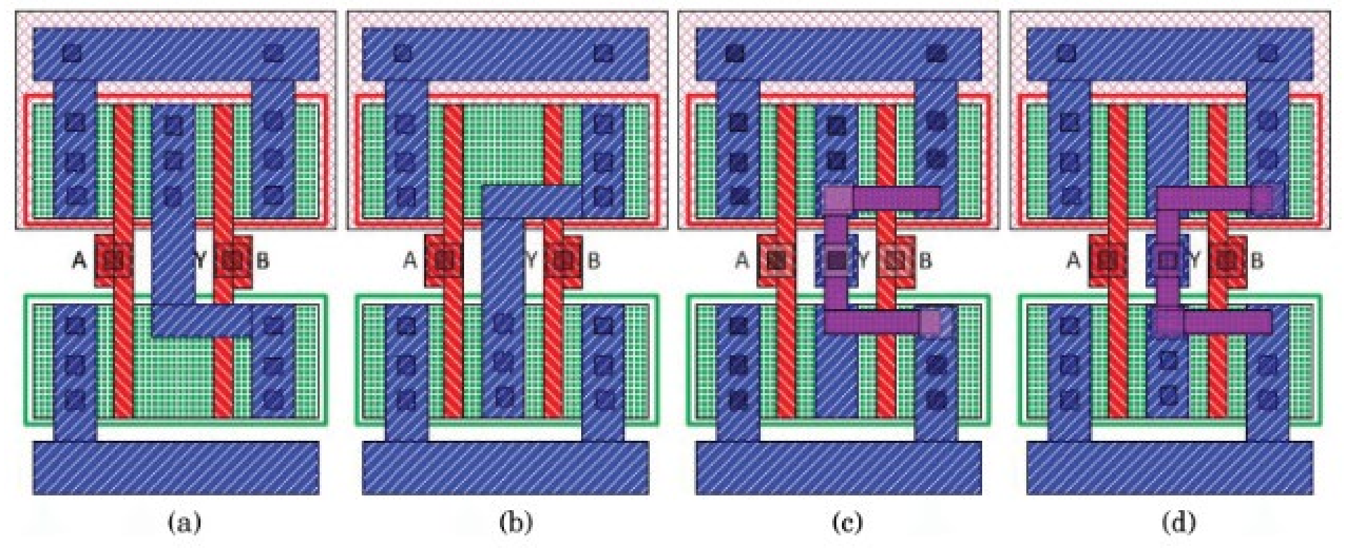


Logic Encryption



Universal Gate (e.g., NAND) Implementation

2. Layout Camouflaging



Standard NAND gate (a) and NOR gate (b). These gates could be easily differentiable by looking at the top metal layers. Camouflaged NAND gate (c) and NOR gate (d). These gates have identical top metal layers and are therefore harder to identify

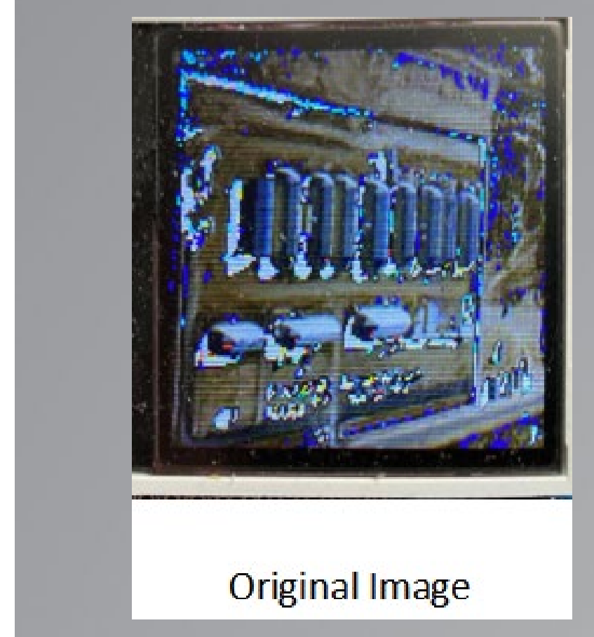
INFORMATION INSTITUTE®

CYB

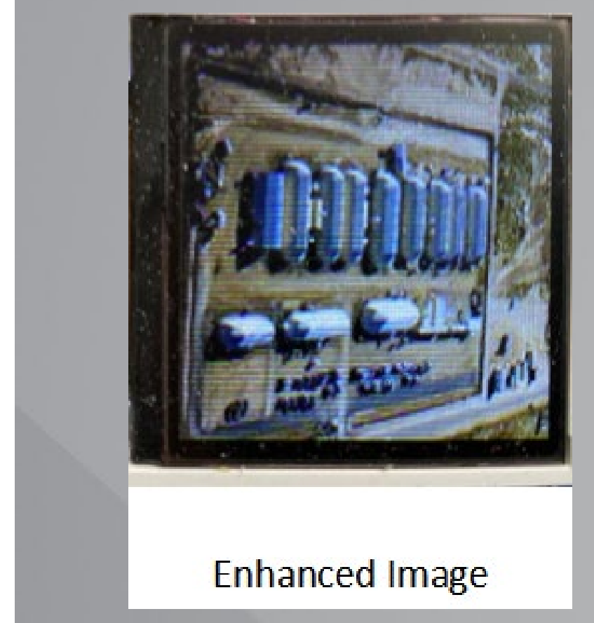
AIR FORCE RESEARCH LABORATORY

INFORMATION INSTITUTE MISSION: Strengthen and expand information technology research, develop collaborative relationships, and increase research emphasis in areas of information technologies for the Information Directorate.

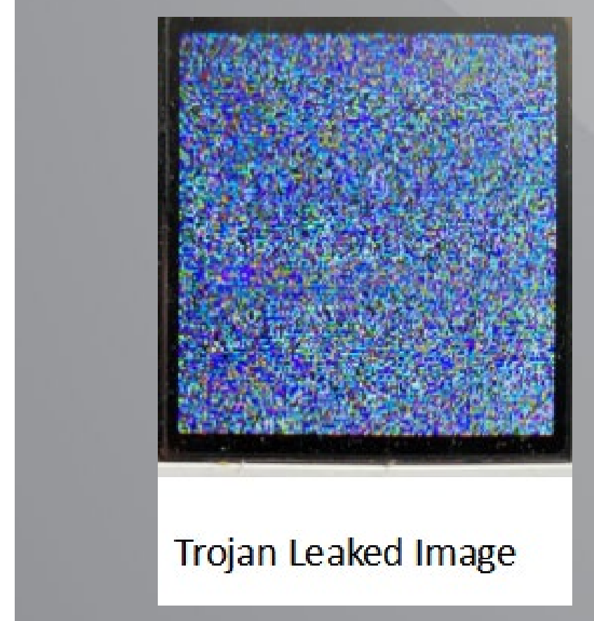
A Platform for a Broad and Diverse Range of Design for Security Techniques: From Chips to Boards



Original Image

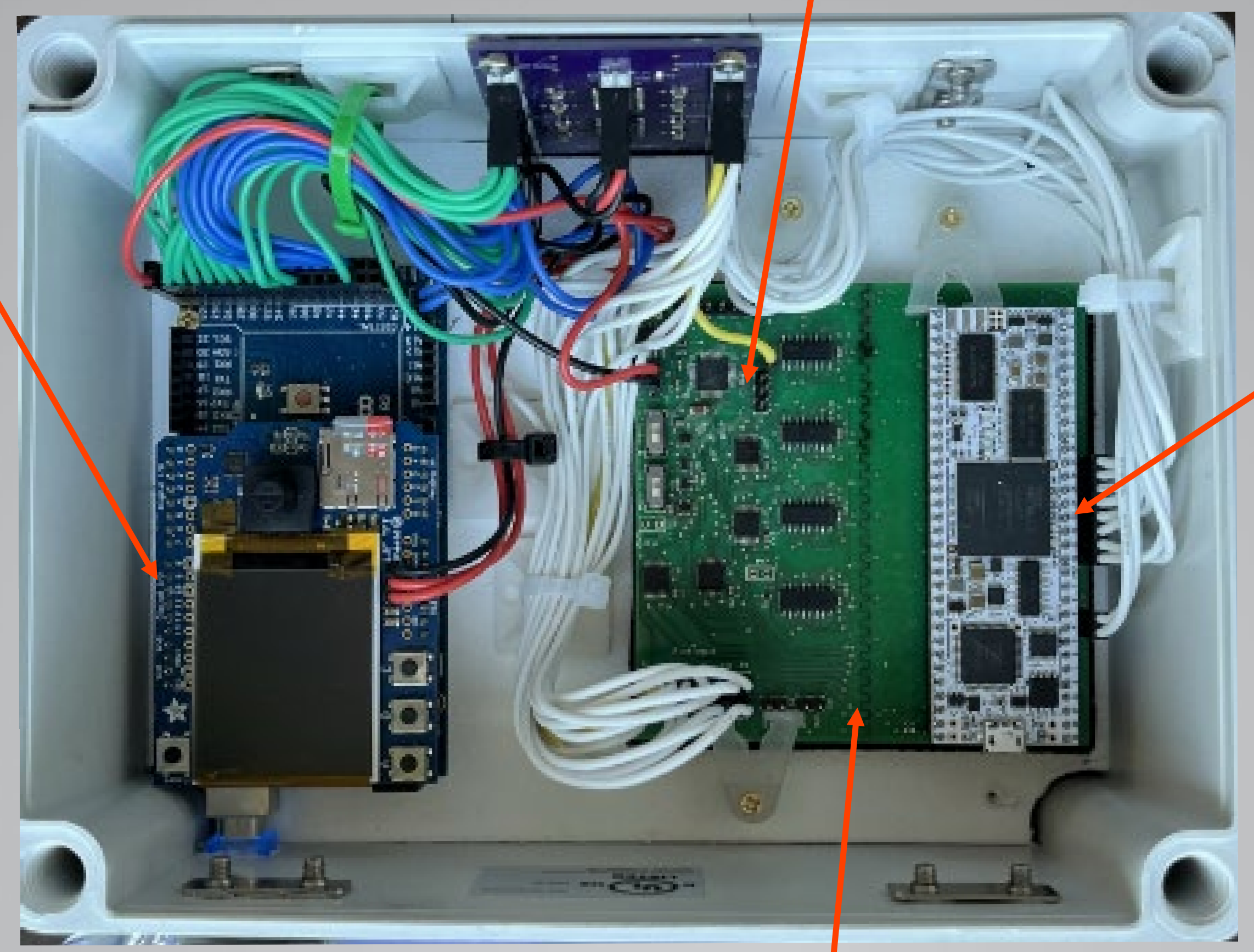


Enhanced Image



Trojan Leaked Image

See demo output

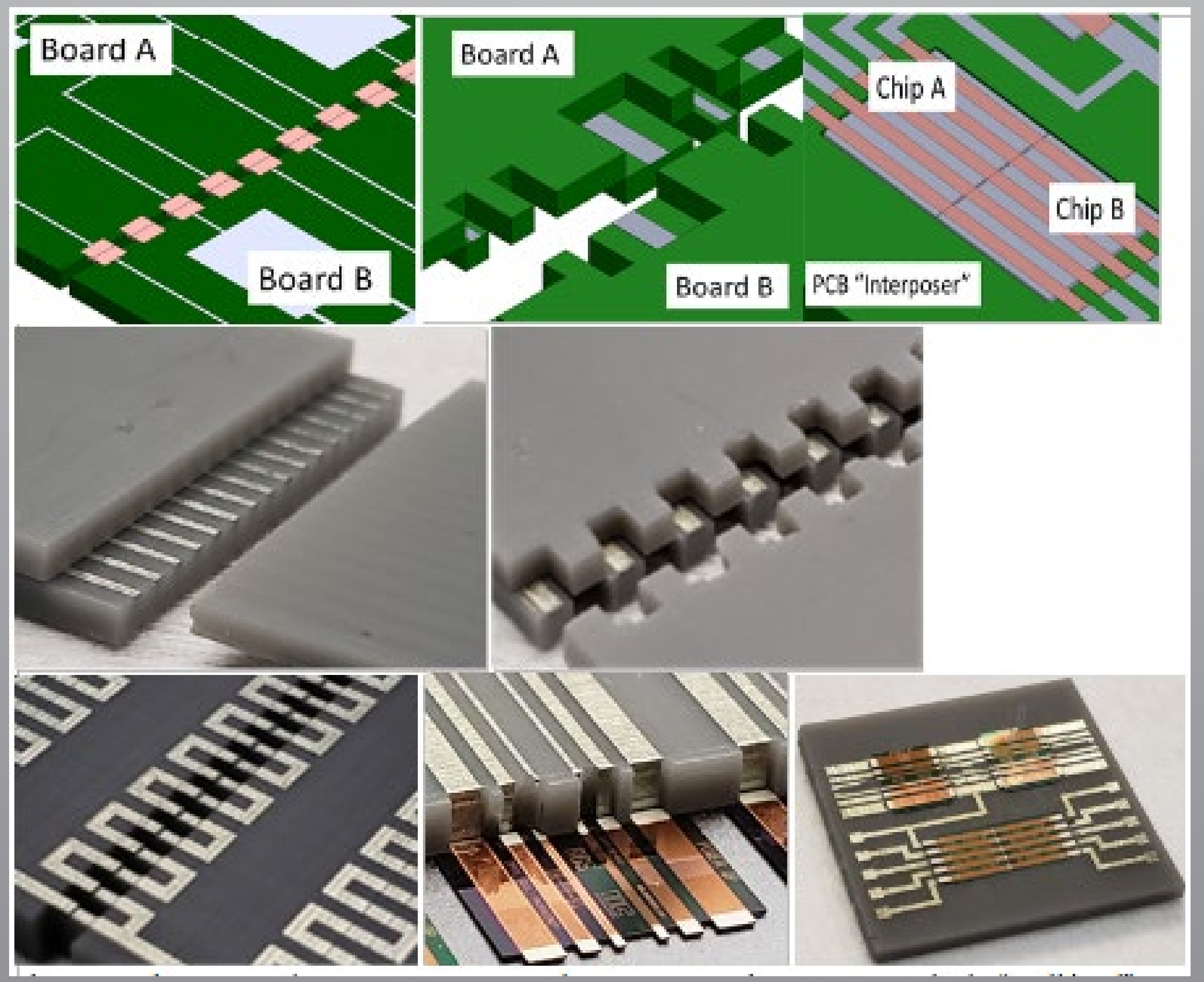


Board with trusted generic I/O modules

Arduino Display unit

Outsourced board with FPGA module implementing RECORDized image enhancement function

Castellation of quilting boards

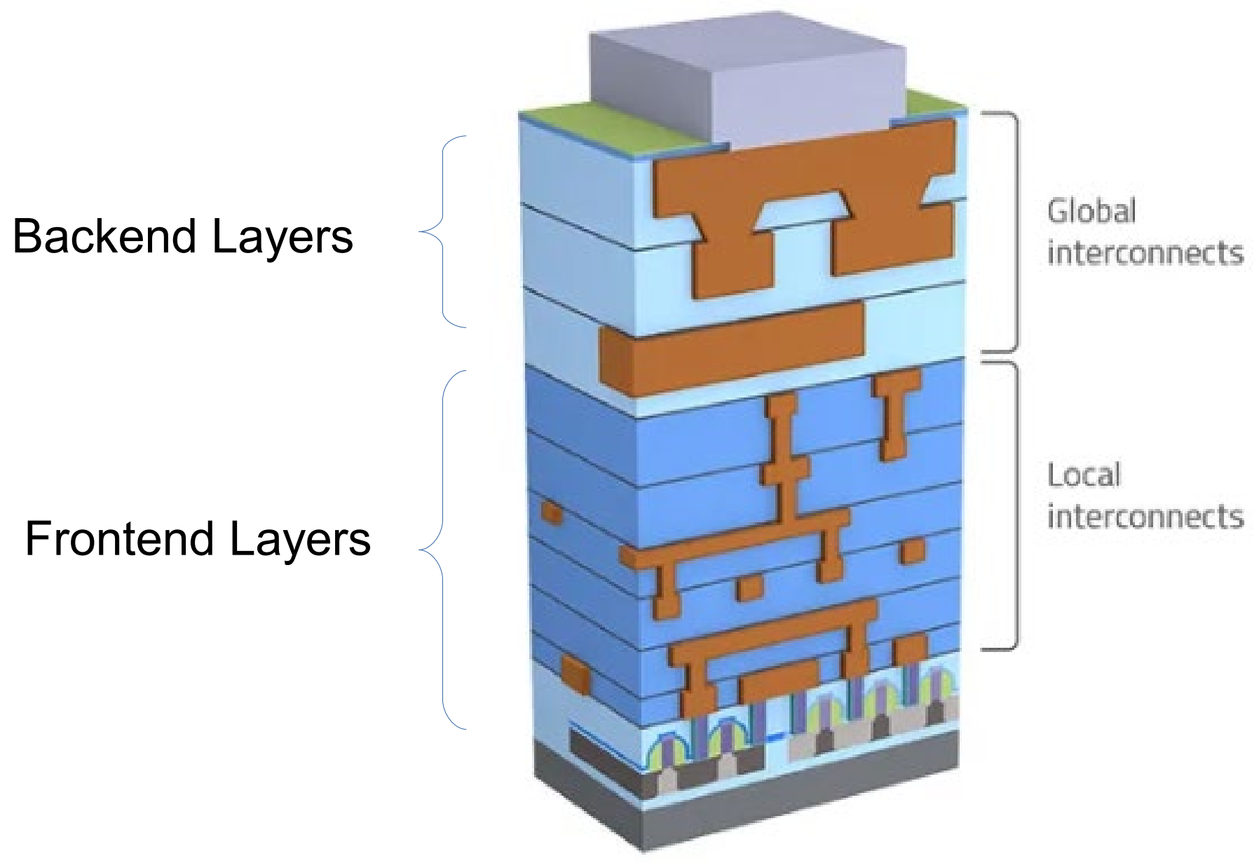


Indiana Integrated Circuits (IIC) licensed Quilt Packaging – a high-bandwidth, low loss chip-to-chip and board-to-board interconnection technology (invented at the University of Notre Dame)

Approved for Public Release; Distribution Unlimited: AFRL-2023-3559

METHODS (Continued):

3. Split Manufacturing



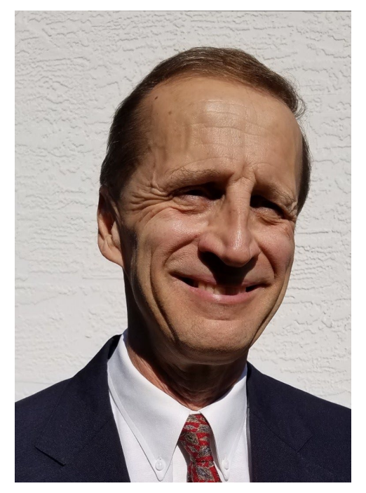
RESULTS:

- The 3 DFS Methods can be defeated if same design is to be manufactured by multiple fabrication runs
- Instead of trying to hide the design from an attacker through any of the existing means, RECORD (**R**andomized **E**ncoding of **CO**mbinational Logic for **R**esistance to **D**ata Leakage) temporarily randomizes the operation of the design
- Keeps supply chain from being disrupted
- RECORD not only admits DFS techniques in the initial fabrication run, but is indifferent to re-introducing them in future runs (if warranted))

ADVANCEMENTS

- Exploring integration of new hardware security technique: reconfigurable FPGA moving target defense
- Continuing synergy-building with AFRL/RI's IoT Living Laboratory
- IIC re-licensed AFRL's RECORD patented inventions for commercialization
- A new RECORD invention is patent-pending
- New licensing action underway with launching of a RECORD-focused start-up
- Key Lake Technologies bringing RECORD to the forefront of hardware security

CAESAR GROUP
Commercial Applications for Early Stage Advanced Research



Kevin Kwiat, PhD, Former AFRL Principal Computer Engineer on an Air Force Science and Technology Fellowship