N65236-10-X-0023: 2.22

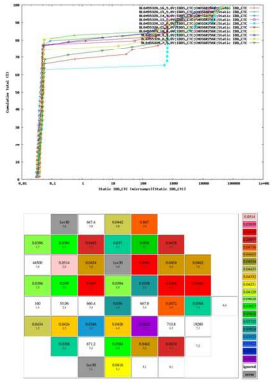
Cyber Warfare and Information Dominance Solutions

Cyber Supply Chain Risk Management

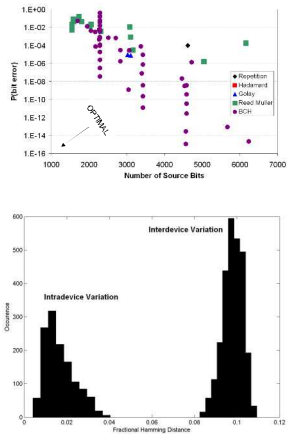
Total Reliability Using Standardization and Test (TRUST)

SAND2010-4973P

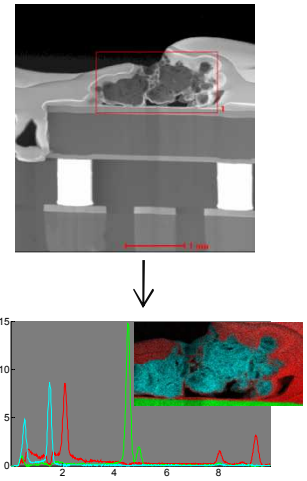
Electronic test-based datasheet fingerprint



PUF Fingerprinting



Attribution example: elemental analysis



Operational Capability

We will provide a full solution that ensures the U.S. Government's supply of microelectronic components is reliable and secure. This system will provide protection and deterrence against counterfeit and subverted components entering the supply stream for critical assemblies. There are three R&D aspects to this proposal built upon the foundation of Open Standards: 1) determination of the feasibility of a tightly specified, multi-variable "data sheet" of characteristic measurements made at the time of manufacture to identify consistently a specific component without specially designed circuitry in the component itself; 2) development of an electronically readable, non-clonable, integrated "fingerprint" circuit that can be placed into a component; and 3) development of sophisticated forensic techniques to identify component origin (attribution of manufacturer).

There are three major reasons why the U.S. Government must lead this effort:

1) Despite widespread recognition of the benefits of standardization within industry, competitive market forces have prevented industry from independently building the necessary standardized test equipment necessary to support counterfeit identification.

2) Adopting a comprehensive solution will impact the U.S. Government's micro-systems concerns across the entire logistics spectrum - weapon system design (i.e. prognostic and autonomic logistics), maintenance activities, modification efforts and sustainment practices.

3) U.S. Government influence in the micro-circuit market sector will be re-established. This time, however, it will be based upon championing innovative technical and supply chain management solutions instead of relying upon a dominant market share in the sector.

Proposed Technical Approach

Overview:

We propose 2 broad tasks to answer these questions: 1) can characteristic measurements be determined carefully enough in the "component enrollment" stage (initial test after manufacture) so that the components can be positively identified in a later "validation stage;" 2) can the means to make these careful measurements be sufficiently portable, fast, and inexpensive to make this technique viable for a wide range of components, 3) can these techniques be combined with Physically Unclonable Function (PUF)-based component authentication so that the full re-measurement validation need not be performed in the field; and 4) can these techniques be combined with certain "chip forensic techniques" to positively identify the source foundry of components that are found to be of uncertain origin?

Task 1: a sample of parts (approximately 100 unmarked), will be tested on identically configured proprietary ATE systems to conclusively prove that counterfeit detection can be accomplished using portable qualification code, i.e. a digital datasheet, which will specify the unique test parameters of each IC type and facilitate the ability to accurately authenticate IC's at various physical locations in a timely manner.

Task 2: traceability will be confirmed through fingerprinting and attribution: 1) Attribution of Commercial Off The Shelf (COTS) IC parts to a specific manufacturer and fabrication facility, or validation that a particular component was not produced in a particular foundry. 2) IC Fingerprinting by demonstrating feasibility of PUFs-based component authentication via JTAG interface using a FPGA platform.

Rough Order of Magnitude Cost and Schedule

Each task will run in parallel and will take 12 months from receipt of funding. Each task will cost approximately $500K for a total project cost of $1M.

Deliverables

Task 1: 1) POC research and demonstration that a universal digital datasheet can uniquely authenticate a previously tested component and 2) description of an ideal open standard test architecture.

Task 2: 1) validation and verification of applicable techniques capable of attributing or dis-attribution of manufacture location of microelectronic components and 2) demonstration, using COTS FPGAs, of a non-reproducible PUFs-based component "fingerprint" to uniquely and non-reproducibly identify a high-value, critical microsystem component to prevent counterfeit or subverted part insertion.

We will report details of the findings and results from all activities in a final project report due at 12 months from receipt of funding.

Corporate Information

ZTI is a small business comprised of industry veterans with over 90 years of semiconductor experience & multiple letters of support for the concept of T.R.U.S.T. ZTI areas of expertise are: ATE architecture design, high-performance instrumentation, test engineering, and consortia management. Sandia National Laboratories is a Department of Energy National Laboratory specializing in solving critical national security needs. MESA (Microsystems Engineering and Sciences Applications) is one of Sandia's largest centers. MESA is responsible for COTS procurement, ASIC design and production (including packaging, test, and failure analysis), and essentially all of Sandia's various microsystems requirements.