



Fact Sheet

Defense Advanced Research Projects Agency

3701 North Fairfax Drive
Arlington, VA 22203-1714

IMMEDIATE RELEASE

December 2007

DARPA TRUST IN INTEGRATED CIRCUITS PROGRAM

Introduction

The worldwide market for integrated circuits has expanded dramatically over the past 50 years to an industry valued at over \$200 billion in 2007, with the majority of this market resulting from manufacturing and sales of commercial products throughout the world. As a result of this globalization, integrated circuit production is rapidly moving off-shore to Taiwan, Singapore, the European Union, Japan, and Peoples Republic of China.

The U.S. military now consumes only about one percent of the total integrated circuit production in the world. Therefore, the military supply requirement is no longer a dominant factor that can influence integrated circuit production. The majority of integrated circuits used in complex modern military systems are made off-shore.

A Defense Science Board study published in February 2005¹ concluded that the offshore production of integrated circuits poses concerns for the United States. The problems described in this study are becoming more acute. The concerns range from reverse International Traffic and Arms Regulations restrictions to the possibility of malicious circuits being inserted into the integrated circuits that are made overseas. At the present time, the United States does not have a comprehensive program to certify that the integrated circuits that are going into U.S. weapons systems do not contain malicious circuits.

DARPA TRUST in Integrated Circuits Program

In response to these concerns, DARPA has initiated the TRUST in Integrated Circuits program to develop technologies that will ensure the trust of integrated circuits that are used in military systems but that are designed and fabricated under untrusted conditions.

The DARPA TRUST in Integrated Circuits program will not rely on procedures, but only trust techniques and testing technologies that can be measured. By basing the degree of trust assigned to an integrated circuit on measurable metrics, the DARPA program makes a radical departure from conventional approaches. Neither metrics for trust nor the testing methods to quantify trust has ever been done before in hardware design and fabrication of integrated circuits. The DARPA program is pursuing a metrics approach that is formulated in terms of probability of detection vs. probability of false alarms. This provides a clear path to identification of an

¹ Defense Science Board Task Force on High Performance Microchip Supply, February 2005, http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf

(more)

integrated circuit that was maliciously attacked. However, DARPA departs from the traditional definition (where the Trojan Horse is the signal) to a more basic measurement where any change in the integrated circuit (e.g., transistor, wire, etc.) is considered the signal. This provides a good “change” basis around which we can define metrics. (As opposed to the unmanageable case where we might be faced with a semi-infinite number of possible Trojan Horses.)

The DARPA TRUST in Integrated Circuits program consists of three one-year phases. The metrics for the program become more difficult in each phase, with the number of transistors examined increasing and the time allowed to perform the examination decreasing. At the same time, the required probability of detecting a change to the integrated circuit increases and the probability of declaring a good circuit as bad decreases.

The performers on this program have been divided up into two basic groups, the government team and the technology development team. The breakdown of the Phase 1 performers and which team they fall under are as follows:

- Government Red Team (Mass. Institute of Technology Lincoln Laboratory lead; \$600,000)
- Government Test Article Team (University of Southern Calif. Information Sciences Institute; \$4,484,286)
- Government Metrics Team (Johns Hopkins University Applied Physics Laboratory; \$940,217)
- System Integrator (Raytheon; \$2,127,000)
- Hardware and Software - Thrusts 1, 2 & 3 (Raytheon; \$11,941,368)
- Field Programmable Gate Arrays - Thrust 3 (Luna; \$4,521,299)
- X-ray Analysis - Thrust 2 (Information Sciences Institute/Xradia; \$2,347,760)

The Government Test Article Team will provide common test platforms, or test articles, on which all performers will be evaluated. These test articles will be representative of designs commonly used today and will feature modified circuits to be inserted by the Government Red Team. The Metrics Team will develop a very comprehensive set of metrics and support the evaluation of the approaches of the technology providers.

The TRUST program technology development team is organized into three thrusts for ensuring trust in integrated circuits:

- Thrust 1 - Ensuring trust in the design cycle for application specific integrated circuits (ASICs).
- Thrust 2 - Ensuring trust when an ASIC is fabricated in an untrusted foundry.
- Thrust 3 - Ensuring trust when employing field programmable gate arrays (FPGAs) in military systems.

The challenges for the program are significant for each of the tasks.

Thrust 1, the design task, is perhaps the most challenging; it might be called the if-and-only-if problem. The present set of commercial design tools focus on making sure the integrated circuit meets all of the required functionality defined in the specification. In general the tools do not

(more)

focus on determining if additional functionality has been added or modified in the circuit design which was contained in the original specification.

Thrust 2 is the foreign foundry-related task. It basically combines destructive and non-destructive reverse engineering technology together to enable detection of circuit modification when an integrated circuit is fabricated in an untrusted foundry. The primary challenges for this task are to drastically reduce the time to perform the destructive reverse engineering and to develop the ability to make effective non-destructive measurements of a non-delayed integrated circuit.

Since FPGAs are becoming the integrated circuit of choice for both commercial and military systems, Thrust 3, the FPGA-related task, is becoming increasingly important. Although domestic-based companies dominate the FPGA sales market, for all practical purposes all FPGAs are fabricated offshore. The design process suffers from the same design vulnerabilities as do ASICs, including the use of offshore, third-party intellectual property. However, the design flow for FPGAs presents additional verification issues since many of the design tools are vendor-specific and highly proprietary.

The TRUST program presently contains many novel techniques and approaches to measure trust. These leverage X-ray tomography, Boolean equivalence checking, physically unclonable functions, electromagnetic probes, simultaneous focused ion beam etching and scanning electron microscope imaging, Graphic Data System II (GDS II) to netlist generation and advanced pattern recognition.

Additional Resources:

- DARPA media contact: Jan Walker, (703) 696-2404, jan.walker@arpa.mil
- TRUST in Integrated Circuits solicitation: <http://www.darpa.mil/MTO/solicitations/baa07-24/index.html>

-END-