RY15-11

AFRL CALL FOR DAGSI Topics

1. **Research Title:** *Cyber Techniques for Design of Trusted Microelectronics*

2. **Individual Sponsor: AFRL/RYW (POC: Matthew Casto)**
Mr. Matthew Catro
AFRL/RYDR Bldg 620
2241 Avionics Circle
WPAFB, OH 45433-7333
Matthew.Casto@us.af.mil

3. **Academic Area and Education Level:** Electrical & Computer Engineering/VLSI and Formal Verification (Ph.D. Level)

4. **Objectives:** The primary objective of this research is to develop a taxonomy of hardware vulnerabilities and fault generators that are representative models of hardware Trojan components potentially inserted into FPGAs and/or integrated circuits. Vulnerabilities will be enumerated and ranked in priority as a vulnerabilities list. Hardware Fault Pattern (HFP) generations of vulnerabilities needs to be developed similar to what has been established for software common weaknesses. With a ranked vulnerability enumeration list developed, techniques of Formal and Testbench Verification may be developed and applied for the purpose of evaluating an FPGA or fabricated integrated circuit's integrity to the original design specification.

5. **Description:** As microelectronics continues to advance in their complexity and to be purchased from varied supply chains, there is an increased concern of integrated circuits containing hardware Trojans (malicious bugs) or fabrication faults that would compromise the integrity of the original chip functionality. Currently, there is not a well-established methodology for verifying that the outsourced golden design accurately represents the fabricated chip. As a result, there is an increasing concern regarding the level of trust one can have in the fabricated chip once it has been received back from the foundry, namely if the chip is fully equivalent to the original golden design. In the same manner that software Trojans were developed out of malicious intent in order to compromise computer systems, hardware Trojans are starting to become more prevalent in the chip manufacturing industry. The varied and sometimes unknown supply chain presents many opportunistic points in the manufacturing flow for Trojan insertion. The scope of the trusted microelectronics research involves developing a taxonomy or classification of hardware vulnerabilities and fault generators and Trojans that can be used to develop statistical fault models. These fault models would then be employed for establishing metrics for evaluating design integrity.

6. **Research Classification/Restrictions:** This work is unclassified; U.S. Citizens only.

7. **Eligible Research Institutions:**
   X Universities (DAGSI) __ AFIT only __ USAFA