RY18-4

AFRL CALL FOR DAGSI Topics

1. Research Title: *Formal Method-Based Microelectronic Assurance Analysis*

2. Individual Sponsor:

AFRL/RYD
Mr. P. Len Orlando
AFRL/RYDI
2241 Avionics Circle, Bldg 620
WPAFB, OH 45433-7333
pompei.orlando@us.af.mil

3. Academic Area and Education Level: Electrical & Computer Engineering or Computer Science Formal Methods, Hardware Verification (Ph.D. or M.S. Level)

4. Objectives: The primary objective of this research is to develop scalable approaches for the use of Formal Methods for digital hardware assurance that provide automatic inspection capabilities for hierarchical blocks of a gate level digital design. Quantification of the portions of the design investigated will be produced along with an enumerated list of the types of structures automatically verified and the degree to which they formally match expectations. Techniques to improve automatic coverage and enhance state space coverage via other traditional digital verification capability may be developed and applied to increase the portion of a design formally verified. Algorithms will be applied to a range of digital design types and styles to explore the capacity of the algorithm to handle various types of intellectual property (IP) blocks commonly used in modern system-on-chip (SoC) designs.

5. Description: A significant increase in the complexity of digital circuits has required new approaches to verification. These new approaches such as Formal Methods can provide high assurance that the intent of a design is preserved throughout the design process without the need to result to exhaustive simulation. Currently, there is a need to be able to inspect third party IP designs from untrusted origin to provide assurance that the blocks perform only the desired function without hidden operations that may compromise a larger SoC design. While Formal Methods can provide a mathematical proof that only the desired function exists in a design, their mathematical approach breaks down in the presence of the state-spaces inherent in modern complex IP blocks. As a result, their application is limited to small portions of a design where the state spaces are highly constrained such as in control flow paths. Enhancements to the capability of Formal Methods via augmented use of traditional digital verification methods in areas of large state spaces have the potential to break through these barriers allowing additional comprehensive verification approachs required to provide assurance for untrusted third-party IP. To ensure scalability of the approach to the wide variety of control and data path types present in modern digital SoC designs, a metric driven approach is highly desirable.

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

7. Eligible Research Institutions:

X Universities (DAGSI) _ AFIT only _ USAF A