The Center for Cyber Defenders

Expanding computer security knowledge

FPGA Authentication

Jeffrey Michaelis, Utah State University;
Zachary Silva, Rose-Hulman Institute of Technology

Project Mentor: Jay Brotz, Org. 6831

Problem Statement:

Field programmable gate arrays (FPGAs) present an opportunity for use in treaty applications where trust is needed by both the host (certification) and the inspector (authentication). FPGAs allow processing tasks to be performed on a platform with a dedicated function (following programming) that also improves power consumption and processing time with respect to general purpose processors without much of an increase in cost. For these reasons, FPGAs may be ideal for use in equipment that must be authenticated.

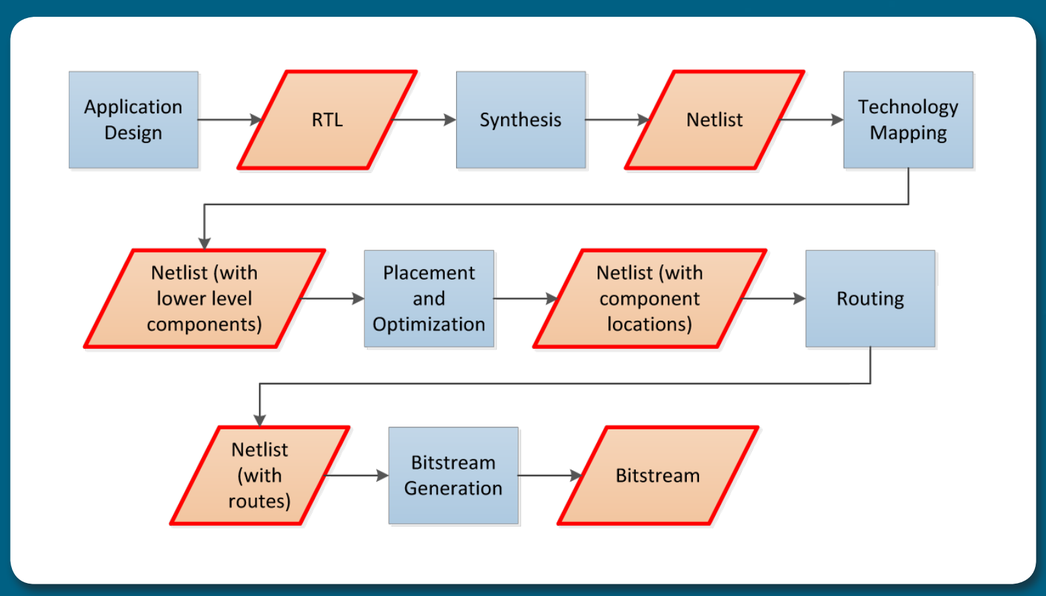

Figure 1: Illustrates areas in the process flow that require authentication.

Objective and Approach:

- Bitstream real time monitor with built-in CRC or hash: Because SRAM FPGAs configure in a synchronous serial manner, real-time monitoring of the configuration data could be accomplished via built-in hashing or cyclic redundancy check (CRC) hardware, which would include the hardware to calculate the hash or CRC and a display to show the result. The result of the hash or CRC will be visually inspectable after configuration completes.
- Functional Simulation Testbench: Functional testbenches are a tool for simulating the behavior of a design to determine the correctness of its logic circuit. Testbenches are user generated designs that apply stimulus to the application and collect output responses. These output responses are then compared to expected values and verified. Source RTL or any synthesized netlists.
- Functional Equivalence Check: Formal equivalence checking is a mathematical technique to prove that two representations of a logic circuit exhibit exactly the same functional behavior, i.e., when stimulated with any valid sequence of inputs, both designs produce exactly the same outputs. Because FPGA designs are a multi-step process whereby the underlying representation of the circuit changes from step to step, formal equivalence checking will ensure that no unexpected logic was inserted into the design or intended logic was removed from it.

Results:

- Functional testbenches verify the code is operational and does what is specified.
- Process of understanding equivalency checking and working to find ways to do it in our design. Working to find ways to implement code that could potentially be malicious and affect the overall functionality. Once this code is introduced, we can compare to the "golden" version and identify the differences.
- Hashing the configuration data and sending the hash to an external display allows a fast easy result in treaty applications, this was tested using a small linux device attached to a seven segment display. It was found that very small hashes could be sufficient in treaty applications.

Impact and Benefits:

This work could be used in treaty application to more thoroughly verify authenticity of FPGAs that are subject to treaties.

The possible benefits of functional equivalence checking and functional simulation testbenches are to increase the depth of current treaty inspections and ease of use for inspections.

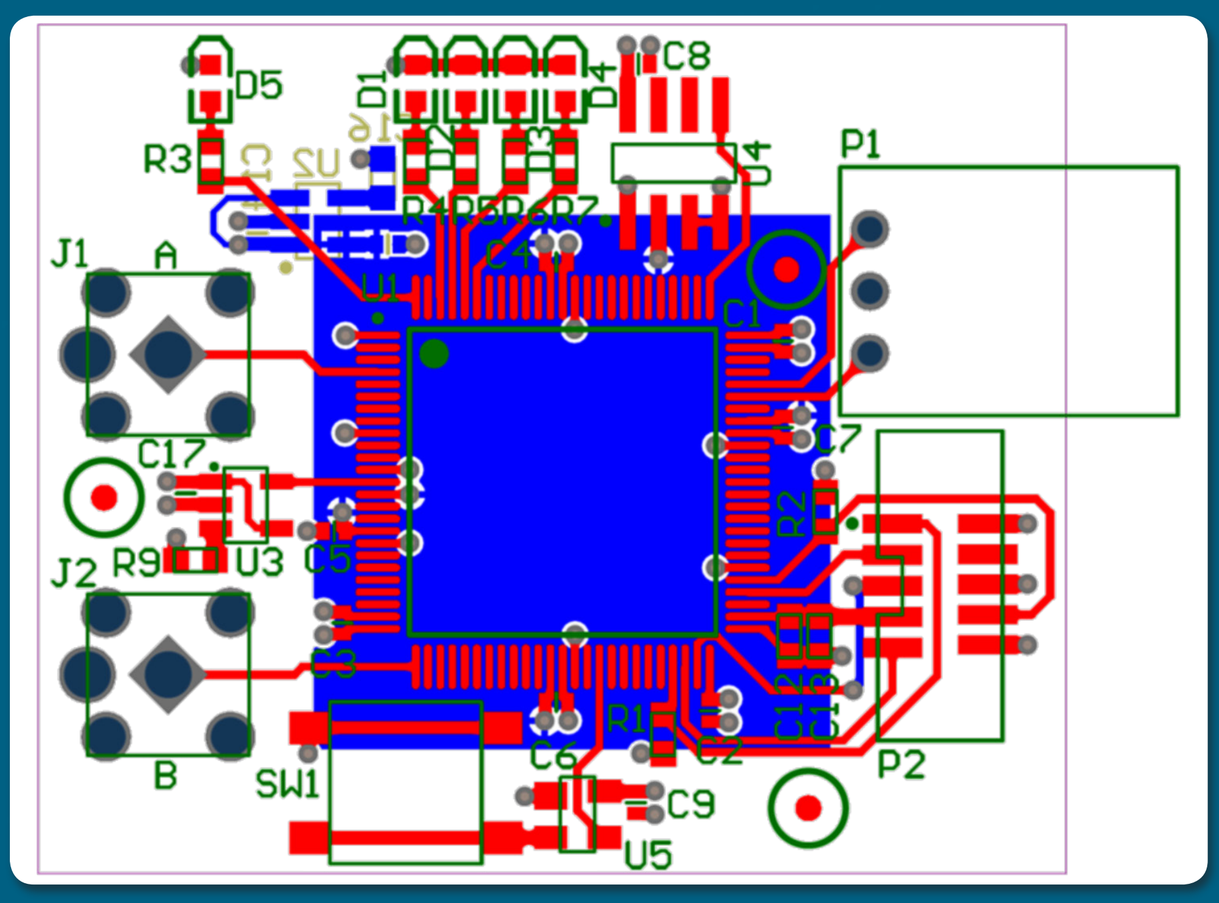

Figure 2: PCB layout used for research and testing.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2016-6899 C.