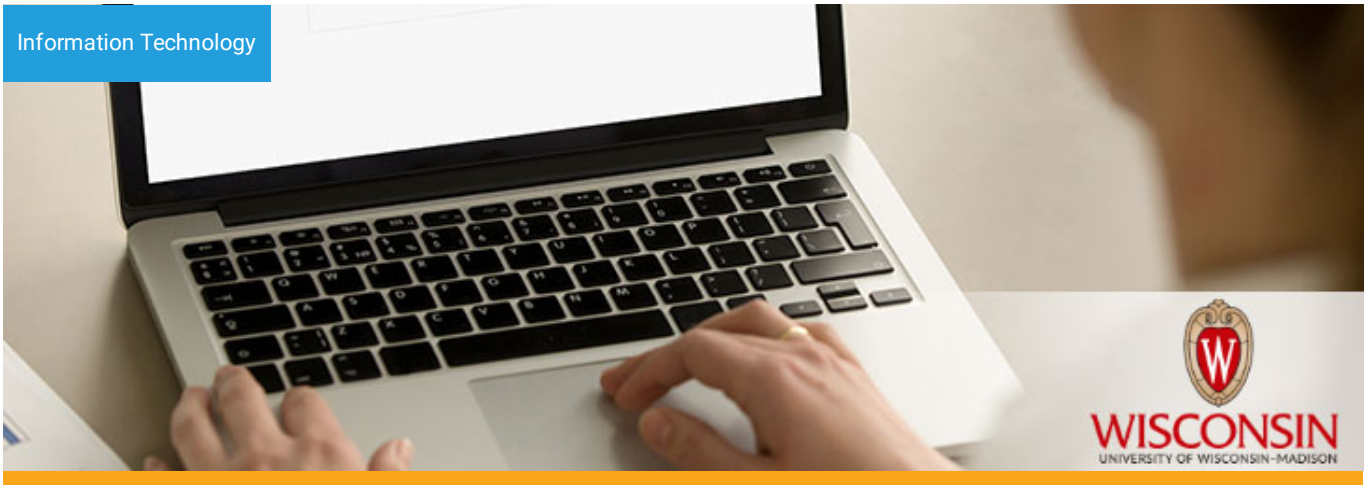
Information Technology



Encrypting Intellectual Property Cores

View U.S. Patent No. 9,390,292 in PDF format.

WARF: P140095US01

Inventors: Parameswaran Ramanathan, Kewal Saluja, Spencer Millican

The Wisconsin Alumni Research Foundation (WARF) is seeking commercial partners interested in developing a method for providing useful descriptions of integrated circuits while concealing their underlying design.

Overview

System-on-Chip (SoC) is a technique for designing complex integrated circuits using circuit 'building blocks' developed by different companies. Electronic files describing each building block are combined and assembled to produce the final product. These building blocks are known as intellectual property (IP) cores, reflecting the fact that their underlying design is sold as opposed to an actual integrated circuit. The ability to license IP cores makes the design of complex circuit elements more efficient and helps share costs among manufacturers.

An IP core can be described in an electronically readable schematic that outlines each component (e.g., logic gates, interconnections and functional descriptions of inputs/outputs). The sale of an IP core may include this entire functional specification, a so-called "soft" core. In contrast, it also is possible to sell a description of an IP core that provides the basic layout but not circuit-level information. This "hard" core allows fabrication of the IP core but hides the circuit design to prevent copying or modification.

The hard core license forms the core of IP vendors' business but it has a major drawback. Namely, because the details are hidden, it is not possible to simulate the IP core with other building block circuits. The ability to simulate is critical for integrating other circuit elements and identifying component faults.

The Invention

UW–Madison researchers have developed a method for encrypting the functional descriptions of IP cores. The encrypted descriptions allow simulation but still obscure the design and operation of the underlying circuit. This provides more flexible testing capabilities while protecting intellectual property.

First, an encryptor receives a description file of the circuit. The encryptor then outputs a description of the underlying IP core in which the nodes or gates of the circuit are replaced with generic placeholder nodes. These placeholders are given encrypted multivalued truth-tables that permit simulation but effectively disguise their function. For example, multiple alias values may hide the logic of the node, or the truth-table may include erroneous entries. The effect is to render the function of the node symbols practically unintelligible.

Applications

- Encrypting digital circuit description files

Key Benefits

- Preserves the confidentiality of circuit designs

We use cookies on this site to enhance your experience and improve our marketing efforts. By continuing to browse without changing your browser settings to block or delete cookies, you agree to the storing of cookies and related technologies on your device. See our privacy policy

OK

- Allows end user to perform simulations
- System works with a large variety of basic circuit building blocks.
- Provides a standard schematic representation
- Simulation is extremely rapid and does not require complex decryption steps.

Stage of Development

The encryption method was used on a test system and performed fault simulation using the most common fault model (single stuck-at-fault). Researchers also tested how long it would take to decrypt the circuit and found that it would be very computation heavy and time consuming.

The development of this technology was supported by WARF Accelerator. WARF Accelerator selects WARF's most commercially promising technologies and provides expert assistance and funding to enable achievement of commercially significant milestones. WARF believes that these technologies are especially attractive opportunities for licensing.

Additional Information

For More Information About the Inventors

- Parameswaran Ramanathan

Related Technologies

- WARF reference number P110103US01 describes a method for hierarchical System-on-Chip testing.
- WARF reference number P06048US describes a method of testing digital circuits that replaces serial scan with random access scan.

Tech Fields

- Information Technology : Computing methods, software & machine learning

For current licensing status, please contact Emily Bauer at emily@warf.org or 608-960-9842

We use cookies on this site to enhance your experience and improve our marketing efforts. By continuing to browse without changing your browser settings to block or delete cookies, you agree to the storing of cookies and related technologies on your device. See our privacy policy

OK