Protecting Designs with a Passive Thermal Tag

Carol Marsh, Tom Kean and David McLaren, Algotronix Ltd and iSLI

ICECS 2008, Malta, 1 September 2008
The Tag Idea

The idea is to provide a tag which can be added to an FPGA, ASIC or IP Core which will uniquely identify that design.

The tag must communicate with external detection equipment via a covert channel.

Aim is to detect IP rather than protect IP.
Why is an ID Tag Required?

Design theft:

Cloning FPGAs from stolen bitstreams

Obtaining designs through fraudulent methods such as bribery or reverse engineering

Dishonest manufacturers ‘overbuilding’ designs and selling the excess to the black market

Customers using single licensed IP on multiple projects
Why is an ID Tag Required?

Falsely marked ‘ghost’ chips:-

- Speed grade changed to increase value
- Date code changed to sell recycled or scrapped chips as new
- Logos changed to sell cheap copies as brand names
Why is an ID Tag Required?

Design recognition:

FPGA package markings identify the FPGA chip, not the user designs within.
Why is an ID Tag Required?

There is a need to recognise:

- FPGA users
- IP Core vendors
- CAD software vendors
Requirements…

FPGA design identification should be just as easy as reading package markings:

- No support from software in the system containing the FPGA is required
- No documentation of chip pin out is required
- Works even when the bitstream is encrypted
- Very low cost

All you need is to be able to see the package lid
Temperature Side Channel

A side channel is a mechanism by which information is leaked from a design and can be measured externally.

A side channel which has not yet been investigated is temperature.

During operation, a design produces heat. As the level of activity changes, the temperature changes. It is therefore possible to deliberately produce heat to generate a signature and to monitor this change in heat.
Temperature Side Channel

**Disadvantage:**
Low data rate

**Advantages:**
No electrical connection required between the heat source and sensor
Difficult to ‘jam’ a thermal communications channel without creating additional power consumption in a chip
Heat sensor can be generated using digital circuits
Introducing DesignTag™

There are 2 types of DesignTag:
An active tag – Heat source within an FPGA continuously outputting a signature which is detected using an external sensor.

A passive tag – Heat sensor within an FPGA which lies dormant until it detects a heat signature from an external heat source.
Active DesignTag™

Three Part Solution:

A small, low power heat generator circuit which is added to the FPGA design

A ‘reader’ which can detect the presence of the tag when held against the chip package

A database of tag codes and corresponding design information
Experimental Set Up

Tag Detection Software

Data Logging Unit and Thermocouple

Spartan 3A Board
Passive DesignTag™

Three part solution:

A small, low power heat sensor circuit which is added to the FPGA design

A heat source which provides the temperature signature

A heat controller which controls the heat source
The Heat Sensor comprises of 5 components.

Heat Detector – contains a circuit which monitors the temperature of the design. Temperature rise wakes up the rest of heat sensor
Heat Sensor

Synchronizer – monitors the incoming heat preamble

Determines the heat signature’s period and produces a sample pulse for use by the decoder
Heat Sensor

Decoder – checks the temperature on each sample pulse.
Getting hotter = binary ‘1’
Getting cooler = binary ‘0’

Extracts the 64 bit code being transmitted
Heat Sensor

Tag Code – Designs own stored 64 bit tag code

Comparator – Compares extracted code with stored code
Match = Response is initiated
No match = No response
Heat source is a Peltier Cooler (Heat pump)
Heat pumps are used to extract heat from a component.
Reversing the current heats up a component.
The heat source is taped to the lid of the FPGA
Heat Controller

In the experiments an FPGA on a Xilinx Spartan 3 Evaluation Board is used as the heat controller.

The FPGA is programmed via a laptop with the required 64 bit tag code.

When tag bit = ‘1’ the heat source is switched on.
When tag bit = ‘0’ the heat source is switched off.
Experimental Set Up

Results

Parameters for Xilinx Spartan 3A:
- Tag size = 225 slices
- Power when active = 0.5mW

Time to detect a 64 bit tag: 16 minutes

Tests Performed:
- 1 tag in a Spartan 3 FPGA – tag detected
- 2 tags in a Spartan 3 FPGA – both tags were detected
- 1 tag added to the Spartan 3A Evaluation Board design - tag was detected
Summary

DesignTag™ uses temperature as its communications channel

Active DesignTag™ uses an internal heat source with an external heat sensor

Passive DesignTag™ uses an external heat source with a small, low powered internal heat sensor in an FPGA

Passive DesignTag™
Advantage: Difficult to detect tag unless the code is known
Disadvantage: Detection time is longer than for the Active Tag
Can only look for one tag at a time, with Active Tag can look for the complete database of tags in one sweep.
Summary

Passive DesignTag™ can be used:

To detect misuse of IP
To detect ‘ghost’ chips
To provide a complete list of designs used in a product
To communicate error information
To detect commercial products created with evaluation tools

DesignTag™ detects IP