Protecting Designs with a Passive Thermal Tag

Carol Marsh[1,2], Tom Kean[1], David McLaren[1,2]

[1]Algotronix Ltd
Edinburgh, UK
carol@algotronix.co.uk, tom@algotronix.com,
david@algotronix.co.uk

[2]Institute for System Level Integration, Livingston, UK
carol.marsh@sli-institute.ac.uk,
david.mclaren@sli-institute.ac.uk

***Abstract*: The theft of electronic designs and in particular Intellectual Property (IP) Cores is problematic [1]. Proving a design has been stolen is difficult if not impossible. A method is required to quickly and cheaply identify electronic designs and especially IP Core designs embedded within larger chips or programmed into Field Programmable Gate Arrays (FPGA). This paper introduces a novel thermal tag which will fulfill this requirement.**

I. Introduction

As the popularity of electronics devices increases, companies are producing products which are smaller, more complicated and cheaper, with a shortened time to market.

In order to meet these goals, companies reuse designs and buy in 'IP Core' components, which perform a specific function. IP Cores can be used in FPGAs and Application Specific Integrated Circuits (ASICs).

Unfortunately, some companies take the cost savings resulting from design reuse a step further and use unscrupulous methods to avoid paying for the IP. FPGA bitstreams can be copied from reputable companies systems and used to make low cost 'clones' of those products. ASIC chip design information can be obtained through fraudulent methods such as bribery or by reverse engineering. Dishonest contract manufacturers may 'overbuild' chips or complete products and sell the excess to the black market.

Another form of IP theft involves falsely marked 'ghost' chips. Ghost chips are chips that are marked as valuable products from a reputable semiconductor company but are actually lower specification devices, cheap copies, recycled chips which were recovered from scrapped equipment or even chips which failed test and were 'rescued' from the scrap bins. Ghost chips are difficult to detect, damage the reputation of reputable manufacturers by causing products to fail in the field and would be unsafe if used in critical applications.

IP Cores which have been legally purchased by companies are also open to misuse either accidentally or through negligence. For example, IP Cores can be used on multiple projects when only a single project licence was obtained or royalties could be under paid through incorrect accounting.. Problems can emerge years after the original license agreement for the IP core was signed when the people familiar with its terms have moved on.

Many schemes have previously been suggested to protect design information – this is not surprising since there are also many places in the flow between the design and production where information can be misappropriated and a single scheme cannot protect against every possible attack. Some techniques attempt to prevent design theft through encryption of FPGA bitstreams [2, 3] or design source code [4]. Other techniques attempt to detect misuse after the fact using watermarking [5], still others address particular problems like overbuilding [6]. Just like a house-owner who fits locks on their doors, installs a burglar alarm and registers high value property in an insurance database it makes sense for IP owners to combine both prevention and detection techniques to increase overall security.

A related problem which FPGA users, IP Core vendors and CAD software vendors face is that, unlike semiconductor companies, they cannot use ink markings on the chip packages to identify which chips contain their IP. This is an issue not only of preventing piracy but also of brand recognition.

The Passive DesignTag™ described in this paper and at greater lengths in the corresponding patent applications [7, 8] provides a method which quickly identifies the IP used in a chip.

The Passive DesignTag™ proposed here differs fundamentally from Algotronix' current DesignTag™ product. Where the DesignTag™ product actively transmits a signal which is detected by an external sensor, the Passive DesignTag™ described here responds to a signal from an external transmitter. Only once a unique code from the external transmitter is detected does the Passive DesignTag™ take any action. The fundamental advantage of the Passive DesignTag™ technology described here is that because it is

inert until its unique code is detected it is extremely difficult for a nefarious party to detect its presence and remove it. The fundamental disadvantage of the Passive DesignTag™ described here compared with Algotronix' DesignTag™ product is that it is necessary to know in advance which tag one is looking for in order to transmit the correct code. DesignTag™, on the other hand will detect any tags present in the 'suspect' chip.

The Passive DesignTag™ can be used for the following purposes:-

- To detect misuse of IP by companies who have legally acquired the design
- To detect fake or 'ghost' incorrectly marked chips
- To allow service engineers to obtain a complete inventory of chips used in a product
- To communicate error information from areas of a design which would normally, be inaccessible to test equipment.
- To detect commercial products which have been created using evaluation or donated educational CAD tool licenses
- To mark chips which contain sensitive technologies in a tamper resistant manner, for example, military technologies subject to export licensing.

II. DESIGN OVERVIEW

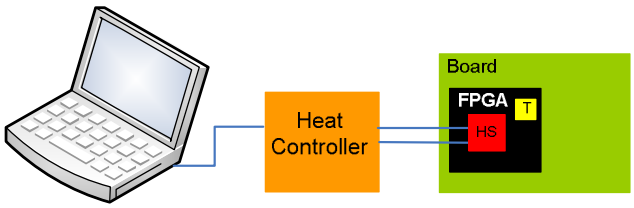

Figure 1. Passive DesignTag™ Circuit

The Passive DesignTag™ system consists of three components, refer to Figure 1: the Passive Tag IP Core itself within the user design to be protected, a heat source applied to the chip package and a heat controller

The passive tag is a small digital circuit which will be incorporated into the design being protected. This tag will contain a secret code which will uniquely identify the design.

The heat source is a device which will supply sufficient heat for the passive tag to detect its presence. It will create a covert channel between itself and the passive tag. Possible heat sources are light bulbs (light bulbs emit significant infra-red radiation as well as visible light and are of interest because they do not require direct contact with the chip package) and resistors.

The heat controller is a programmable device which is used to switch the heat source on and off in a predetermined sequence. A laptop computer is used in the experimental setup to program the required sequence into the heat controller.

To check if an IP Core is present in a design, an agent (for example an employee of the company providing the tag or a police or customs officer) will place the heat source on the device they are checking then they will program the heat controller with the tag code they are trying to detect. If the tag is present a response will be generated – the exact form of the response is design dependent. In the simplest case the design might simply turn itself off. If there are several tag codes in a design, only the tag code being checked for will reply.

Note that the present implementation of the Passive DesignTag™ technology is not suitable for use on a device which has a heat sink fitted to it although, in principle, future versions could do so.

The design goals for the passive tag IP Core were that it should be a digital circuit (to allow use on FPGAs) with low area and power consumption and that it must be difficult for an adversary to find and disable.

III. THE DESIGN

A. Temperature Side Channel

A 'side channel' is a mechanism by which information is leaked from a design and can be measured externally. The most common 'side channels' are Timing [9], Power Analysis [10] , Electro-Magnetic Analysis [11] and Fault Analysis [12].

A 'side channel' which to the best of our knowledge has been largely ignored is Temperature.

During operation, a design produces heat. As the level of activity in a design changes, the temperature will change and thus it is possible to extract information about the design.

In the same way it is also possible to deliberately produce heat using a heat generator to send a message via a temperature side channel and capture this message using a heat sensor. This paper introduces such a scheme.

The disadvantage of using temperature as a communications channel is its low data rate. It takes time to heat up a chip package and even longer for it to cool down again. However for the Passive DesignTag™, only around 64 bits of data needs to be transferred. Moreover, it is acceptable to take several minutes to transfer the tag data since the alternative method of detecting IP within a chip would be to extract the chip from a system and send it to a laboratory for analysis.

The advantages of using temperature as a communication channel are:-

1. There is no need for an electrical connection between the heat generator and sensor circuits – the transmission can pass through the chip package
2. The heat sensor circuit requires only a small amount of digital logic.
3. It would be difficult to attempt to 'jam' a potential thermal communication channel using on chip circuitry without creating undesirable additional power consumption in the chip.

B. *Passive Tag*

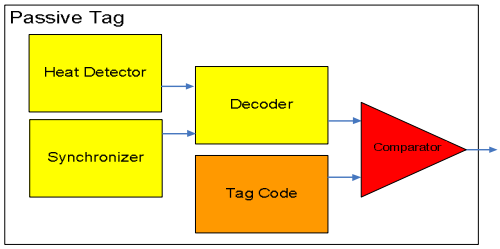

Figure 2. Passive Tag

The passive tag IP Core as shown in Figure 2 comprises of five main components: heat detector, synchronizer, decoder, tag code memory and comparator

The heat detector continually monitors its environment to determine if there has been a rise in temperature. If a rise in temperature is detected for a specified period, the remainder of the tag circuit is activated.

The synchronizer monitors the initial incoming 'heat bits' signaled as temperature changes. This 'preamble' signal has a known form which allows the synchronizer to determine the bit timing period for the message being transmitted. The synchronizer is then able to generate sample pulses synchronized to the incoming data stream, which are used by the decoder.

The decoder on each sample pulse, checks the temperature and determines if the heat circuit is on, which corresponds to a binary '1', or off, which corresponds to a binary '0'. The coding is based on changes in temperature – 'getting hotter' or 'getting cooler' rather than absolute temperature. Using this method the decoder is able to extract the code being transmitted by the external heat generator and convert it into a binary number. This 'tag code' is a 64 bit code, which uniquely identifies a design.

The comparator compares the extracted code with the tags own stored tag code. If there is a match, a response is initiated otherwise the tag remains completely inert and does nothing to give away its presence.

C. *Heat Source*

The heat source is an external device which has to be placed as close as possible to the device under investigation.

The heat source has to provide sufficient heat for the internal passive tag to detect it, while at the same time ensuring that the device under test stays within it operational temperature range.

Three devices were considered as a heat source: a light bulb, a resistor and a Peltier Cooler.

The temperatures produced by the light bulb were too high which led to excessively long cooling times in the transmission waveform.

The resistor produced a good temperature range on the surface of the resistor, however, this was not conducted effectively through the chip package.

The Peltier Cooler, produced the lowest temperature range, however, this was conducted through the package and the tag could easily detect the change in temperature. This is most likely due to the Peltier Cooler having a large surface area compared with the resistor and being in contact with more of the top surface of the package. Therefore, a Peltier Cooler is currently being used as the heat source (a Peltier cooler can either cool or produce heat depending on the polarity of the voltage applied).

D. *Heat Controller*

The heat controller in the experimental setup is implemented using an FPGA on an evaluation board programmed from a laptop computer. It is preloaded with the 64 bit tag code for the design it is trying to detect.

The tag code is converted into a binary sequence which is used to switch on and off the heat source.

When the binary sequence is set to '1', the heat source is switched on and the temperature of the device rises.
When the binary sequence is set to '0', the heat source is switched off and the temperature of the device falls.

The period of the signature code is typically 15 seconds, which means that it takes approximately 16 minutes to send the entire 64 bit signature.

E. *Passive Tag Parameters*

The passive tag requires very little area and power. Table 1 provides the size in terms of slices and the power required when a passive tag is implemented in a Xilinx Spartan 3A XC3S700A-4 FPGA.

TABLE I. PASSIVE TAG PARAMETERS

Chip	Slices	RAM Blocks	Average Power
Spartan 3A	225	0	0.5 mW

IV. EXPERIMENTAL RESULTS

Figure 3. Experimental Setup

Figure 3, shows the experimental set up which was used to demonstrate that the Passive DesignTag™ technology works.

The passive tag was inserted into a design in a Spartan 3A XC3S700A FPGA on a Xilinx 3A Evaluation Board. The design was the Xilinx demonstration design provided with the Evaluation Board. It can be viewed as a typical SoC design and makes use of several large IP blocks including a PicoBlaze soft core processor, a VGA driver which displays messages on a VGA and an audio driver which outputs an audio message to speakers.

A Xilinx Spartan 3 XC3S200 FPGA on a Xilinx 3 Evaluation Board was used as the heat controller. This was connected to a laptop computer via an USB port to allow the tag code to be downloaded.

Since the current drive strength of the FPGA outputs is very low (maximum of 24mA) a Darlington driver on the small daughterboard was required to boast the current to drive the heat source.

A Peltier Cooler was used as the heat source. This was attached to the top of the Spartan 3A FPGA.

V. CONCLUSION

This paper introduces a novel patented technology which uses temperature as the communications channel.

The Passive DesignTag™ comprises of a very small, low powered passive tag, which is added to a design, a heat source and a controller. The Passive DesignTag™ aims to detect rather than prevent the misuse of IP.

It can be used to address misuse scenarios such as, overbuilding by licensed customers, misuse of CAD tool licenses and identifying falsely marked chips which cannot be detected using current techniques.

The Passive DesignTag™ when compared to the current Active DesignTag™ product has the advantage that its passive nature makes its presence extremely hard to detect for anyone who does not know the code. However, it has several disadvantages: detection time is much longer and it is necessary to know which specific tag you are looking for in advance.

REFERENCES

1. Pecht, M. and S. Tiku. *Electronic Manufacturing and Consumers Confront a Rising Tide of Counterfeit Electronics*. 2006 [cited 14 March 2008]; Available from: http://www.spectrum.ieee.org/may06/3423.htm.
2. Kean, T., *Secure Configuration of an FPGA*, in *FCCM 2001*. 2001, IEEE Xplore, pp 259-260: Rohnert Park, California.
3. Kean, T., *Cryptographic Rights Management of FPGA Intellectual Property Cores*, in *Tenth ACM International Symposium on FPGA*. 2002, ACM: Monterey, CA.
4. Ashenden, P., *LCS-2006-140 VHDL IP Protection / Encryption Proposal*. 2006.
5. Newbould, R.D., et al., *Watermarking IC for IP Protection*. Electronics Letters, 2002. **38**(6): p. 272-273.
6. Certicom. *Certicom Security for Fabless Semiconductor Design Companies*. 2006 [cited 14 March 2008]; Available from: www.certicom.com/download/aid-603/AppNotes-fabless.pdf.
7. Kean, T., *Method of Actively Tagging Electronic Designs and IP Cores* in *Unpublished Patent Application: GB 0617697.8*, Algotronix, Editor. 2006.
8. Kean, T., *Thermal Active Tag for Electronic Designs and IP Cores*, in *Unpublished Patent Application: GB0624364.6*, Algotronix, Editor. 2007: GB.
9. Kocher, P., *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*, in *Crypto 1996*. 1996, Springer-Verlag, Volume 1109 of LNCS, pp 104-113.
10. Kocher, P., J. Jaffe, and B. Jun, *Differential Power Analysis*, in *Crypto 1999, 19th Annual International Cryptology Conference*. 1999, Springer-Verlag, Volume 1666 of LNCS, pp 388-387: Santa Barbara, California.
11. Gandolfi, K., C. Mourtel, and F. Olivier, *Electromagnetic Analysis: Concrete Results*, in *CHES 2001*. 2001, Springer-Verlag, Volume 2162 of LNCS, pp 251-261: Paris, France.
12. Bar-El, H. *Introduction to Side Channel Attacks*. [cited 14 March 2008]; Available from: http://www.discretix.com/PDF/Introduction%20to%20Side%20Channel%20Attacks.pdf