



David McLaren
Research Engineer



Algotronix - Overview

Spin out from Xilinx in 1998. Encryption IP Cores and Design IP Protection.

- Advanced Encryption Standard IP Cores
- Patent licensing – FPGA bitstream security
- **New Product** - DesignTag





Encryption Products

- Leading implementation of AES, around 50 design-ins, used by many of the largest defense suppliers also casino gaming, networking, test equipment....
- Highly configurable through VHDL generics to trade area/performance/features
- G3 product addresses full performance range – ultra small with 8 bit data path to ultra-high performance with 10, 128 bit data-paths in parallel. Multi-project licences are particularly cost effective since one product meets every requirement
- Galois Counter Mode (AES-GCM) up to 10Gbit/sec on FPGA while handling minimum sized packets
- Low cost source code access for security review
- G2 product has NIST validation certificate





DesignTag Features

Active tag circuit added to chip design – DesignTag is **NOT** ink on chip package, optically recognised marks on die, or annotations in design source code

- Low Cost Solution
- No electrical contact to chip pins required to scan tag
- Purely digital circuit – no antenna, inductors or special process steps
- Difficult for unauthorised person to detect, tamper resistant
- Identifies the chip directly – detects fraudulently labelled products or chips where original labelling has been removed by the customer
- Low Area and Low Power
- Readable quickly and non-destructively – no need to de-package chip and use microscope
- Tags link to database to provide information on tagged products
- Tracks field-upgrades to FPGA bitstreams





DesignTag Applications

- For Standard Product and Memory Chips
 - Detects falsely marked (rebranded or changed speed/temperature grade) chips in the supply chain
- For IP and CAD Tools
 - Detect unlicensed use
 - Confirm product version
 - Obtain status information
- For FPGA Designers
 - Detect copied bitstream in competitor product
 - Confirm design version and authenticity
 - Add customer ID or serial number for tracking sensitive designs





How DesignTag works

- The tag communicates with the external reader by varying its activity level to cause minute changes in the temperature of the chip package
- Chip packages are designed to be 'transparent' to heat making this a very practical signalling mechanism
- Package temperature changes are around 0.1 deg C and less than random temperature variations
- Spread spectrum code allows tag signal to be extracted from noise
- Thermal signalling is slow but in this application very few bits must be transferred



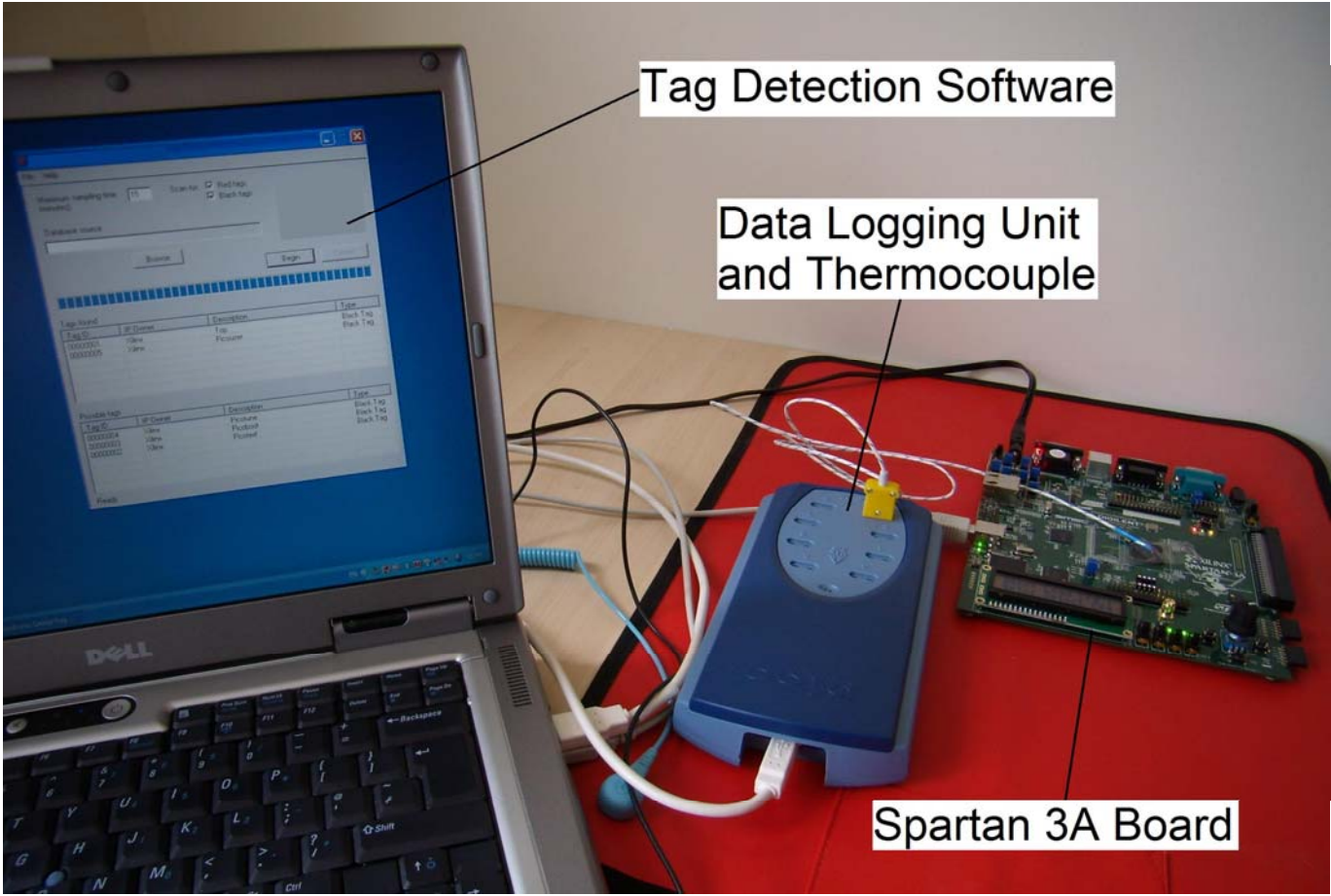


The DesignTag IP Core

- Chip package temperature is modulated by switching on and off a digital 'heat generator' circuit. Low power consumption because only very small temperature changes are required
- Spreading code to control the heat generator is generated using a Linear Feedback Shift Register type circuit based on a 'Tag ID' which acts like a cryptographic key. Each key will result in a different pseudo-noise sequence
- Without knowledge of the key it is difficult for an attacker to distinguish the tag signal from thermal noise. The amplitude of the thermal signal from the tag is below that of random thermal noise
- Product includes countermeasures against removal and reverse engineering



DesignTag in use





DesignTag – Example Use Case

Five tags added to major functional units on a Xilinx SoC design using PicoBlaze processor and running on a Spartan FPGA

- Each DesignTag™ requires 152 slices, 0 RAM blocks
- 5mW additional power per tag when operating, switched off 15 min after power on
- Time to detect tags depends on number of tags in FPGA and location where experiment is run
- Roughly 3 min to find first tag, all five tags found in less than 10 min



Thank you



- Explore Algotronix' IP at ChipEstimate.com
- Use Algotronix' IP to plan your next chip!
- Please stay and talk with David or ask for a demo!

