TECHNOLOGY IMPACT REPORT

DesignTag

Thermal identification of electronic-design intellectual property

2007 public demonstration	**2008** customer launch	**16 files** specialist coverage archive

Purpose

This report records the technical and industry impact evidenced by contemporary coverage of DesignTag. Its subject is the technology rather than an individual award recipient. The IET and NMI awards are relevant as later independent validation, but the main evidence here concerns the problem addressed, technical approach, public demonstration, product launch and industry communication.

What DesignTag was

DesignTag was a small, low-power digital IP core embedded within an FPGA or integrated-circuit design. It generated a minute, coded thermal signal by modulating power consumption. A thermocouple placed against the chip package detected that signal; reader software decoded it and used the tag identity to retrieve information from a database. This allowed a working packaged device to identify protected design content without reading the FPGA bitstream or opening the package.

Problems addressed

• Identifying the design loaded into an FPGA, which conventional package markings do not reveal.

• Providing evidence of ownership when designs or IP cores were copied or used outside licence terms.

• Helping identify counterfeit, remarked or falsely labelled semiconductor devices.

• Recording product version, configuration or internal status through an externally detectable tag.

Technology-to-product progression

2007 - demonstration: DesignTag was announced and demonstrated at the 44th Design Automation Conference. Contemporary reports described Red Tag for product identification/version control and Black Tag for covert IP tracking and licence protection.

2008 - customer launch: The thermal active-tagging system was released with the IP core, reader software, data-logging hardware and database support. Coverage reported around 200 FPGA slices, approximately 5 mW while active, code licences, reader pricing and a starter kit.

Impact evidenced by the archive

Technical novelty

Specialist publications repeatedly highlighted through-package thermal signalling using an all-digital embedded core.

Productisation

The evidence documents a clear move from conference demonstration to a packaged system offered with licences, software, measurement hardware and support.

Defined use cases

Coverage consistently identified FPGA configuration, IP ownership, licence enforcement, counterfeit detection, product revision and status reporting.

International specialist reach

The story appeared across FPGA, semiconductor, electronics-design, automotive and Asian technology channels.

Third-party validation

The subsequent 2008 IET Electronics and NMI Emerging Technology awards reinforced the credibility of the same technology.

Research contribution

The technology was based on collaborative EngD research with iSLI and the University of Strathclyde. Carol Marsh designed and demonstrated several variants, but the report’s principal subject is DesignTag itself.

Evidence boundaries

The archive demonstrates technical communication, specialist-media interest, public demonstration, product launch, pricing, integration with commercial test hardware and external awards. It does not contain reliable sales, licensing, revenue, customer-adoption or long-term deployment figures. This report therefore describes evidenced industry visibility and productisation without claiming commercial scale that the source material cannot prove.

Handling duplicated coverage

Several publications reproduced or closely adapted the same release. One representative copy is included for each duplicated story and all other known publication destinations are listed, preserving reach without repeating identical pages.

Verified working links

Algotronix - DesignTag and research

University of Glasgow - EngD thesis record

EE Times - Two awards for Algotronix

Carol Marsh - Awards & Recognition

Evidence guide

1. The intellectual-property problem: “Mine All Mine”

Independent industry context on electronic-design IP protection, including Algotronix’s work on IP tagging and detection.

2. DesignTag demonstration at the 44th Design Automation Conference

Evidence of a public technology demonstration in 2007 and of the original Red Tag and Black Tag product concepts.

3. EE Times: wireless DesignTag for IP cores

Independent specialist coverage explaining through-package detection, multiple tags, database lookup and access control. **Also published as:** Wireless Net DesignLine - Algotronix offers Wireless DesignTag for IP Cores.

4. Commercial launch of the DesignTag system

Evidence that the technology progressed from demonstration to customer release, with reader hardware/software, technical resource figures, pricing and defined application markets. **Also published as:** SOCcentral - Algotronix Launches DesignTag.

5. FPGA Journal: DesignTag system and product positioning

Specialist FPGA coverage of the thermal signature, watermarking proposition, Red and Black variants, licence pricing and starter kit.

6. EE Times: thermal signalling added to DesignTag

Detailed reporting of the working principle, the roughly 5 mW thermal modulation, the FPGA product and planned ASIC/ASSP application. **Also published as:** Automotive DesignLine - Algotronix Adds Thermal Signaling; EE Times Asia - DesignTag Digital Core Adds Thermal Signaling; ECNMag - IP Core Watermark Technology Protects Chip Designs; New Electronics - Put a Tag on It.

7. When the chips are down: beating the counterfeiters

A distinct product-oriented article framing DesignTag against counterfeit chips, cloned designs and IP theft.

8. How to defend against the cloning of FPGA designs

The most substantial technical article in the archive. It explains the threat model, proof-of-theft concept, implementation cost, detection method and applications in detail. **Also published as:** Digital Home DesignLine - How to Defend Against the Cloning of your FPGA Designs.

9. Pico Technology newsletter

Supplier-side evidence that the DesignTag reader used a Pico Technology thermocouple data logger, showing integration with commercially available measurement hardware.

Reproduced evidence

The following pages are copies from the supplied archive. Historical URLs visible in the copies may no longer work; the saved pages remain the evidence record.

EVIDENCE 1

The intellectual-property problem: “Mine All Mine”

Why it is included

Independent industry context on electronic-design IP protection, including Algotronix’s work on IP tagging and detection.

Mine, **all mine!**

IP is a valuable asset in today's knowledge economy. So how can you protect it? By **Vanessa Knivett**.

Intellectual property (IP) comes in many shapes and forms – patented inventions, copyrighted material, trademarks to reinforce brand identity, proprietary designs that determine product appearance, trade secrets or company specific 'know how'.

The term can refer specifically to internally developed design blocks or cores licensed from an IP vendor to form part of a system on chip (SoC) design. Under the umbrella of intellectual assets, IP might represent one part of a combination of tools and prior knowledge necessary to engineer a new product.

Shorter time to market requirements and the huge number of transistors available nowadays ensure that no matter what the design environment – system or SoC – a level of design reuse is likely to be taking place. Any successful reuse based model relies upon cooperation and trust between engineers, as knowledge of intimate design details such as the RTL HDL source code has to be shared. Meanwhile, with design, test and manufacturing environments now seldom centralised, IP needs to be shared across borders, making it difficult for those charged with protecting it to monitor where it is and who has access to it.

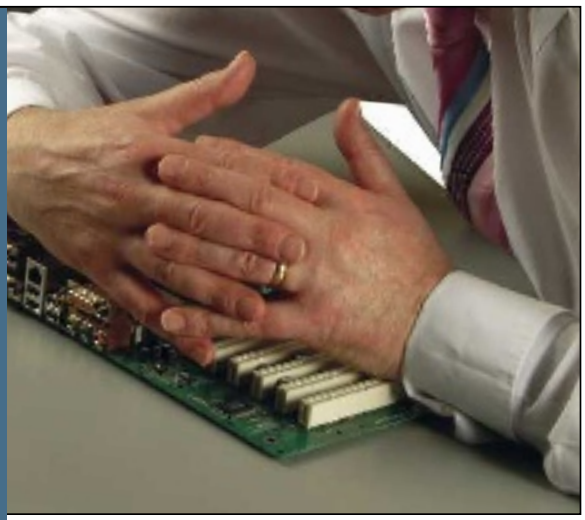
Whatever the form of IP at your disposal, the ability to quantify, qualify and protect it makes good sense. Just as an externally sourced design has a price tag, so internally developed IP needs a value and the appropriate security.

Notes Christian Heidarson, Gartner's lead analyst for IP: "For a company that operates in emerging markets, the most significant threat to its intellectual capital is that of IP diffusion, not IP misuse. IP diffusion happens when key employees leave for another company, taking with them valuable knowledge and customer relationships. This can be entirely legal, as long as the employees don't bring

with them any proprietary designs." Ensuring the appropriate non compete and non disclosure agreements in employment contracts is a start.

Precious IP is likely to be supplied in a more usable form to a contract manufacturer. The migration of contract manufacturing to lower cost economies may have fiscal advantages, but an unproven supply chain can expose IP to misuse. Confirms Heidarson: "Using design and manufacturing services exposes a company's IP to third parties that are often based in countries with weaker legal systems than US and European companies will be used to."

Though there are many reputable contract manufacturers in lower cost regions, IP theft there is believed to be rife. Notes Heidarson, who is based in China: "The legal framework is solid and modelled on British IP law. Enforcement is the problem, as courts still lack experience and the responsibilities of officials remain murky."



"IP diffusion happens when key employees [take] with them valuable knowledge and customer relationships."

Christian Heidarson, **Gartner**

One source of IP theft is overbuilding, where an unmonitored manufacturer builds more product than ordered and then sells them on the local black market. Heidarson advises: "The most powerful and most common strategy for protecting IP is only dealing with companies that you trust. This is because technological solutions for protecting IP make the IP less flexible in the design process and can be overcome by a party determined to do so."

For IP theft is just as likely beyond the manufacturing stage, through cloning, whereby a competitor copies a product, or through reverse engineering to steal the actual design. The latter is more common with analogue technologies, which tend to make use of more mature processes. The problem with this type of IP misuse is that it serves to devalue the original technology, as none of the subsequent products will reflect the cost of the engineering effort that went into the original.

Anti theft strategies

Popular strategies to deter IP thieves include making products difficult to copy using techniques such as encryption, compartmentalising production so different parts of a product are made by different companies, and ensuring that key technologies are kept in countries with robust legal systems.

Most recently developed IP theft deterrents are being implemented within the SoC community. Many of these techniques are based on rendering certain design elements as unique and thus easier to detect when they are misused, for example through tagging and tracking mechanisms, the use of digital signatures or digital fingerprinting, digital watermarking or noise fingerprinting. The reality is that, for IP core vendors, it's customers who can perpetrate IP misuse by using cores incorrectly.

Ironically, for companies keen to detect where their silicon IP is being used, it may mean adopting the skills of the IP pirate. Dr Tom Kean, managing director of Algotronix, explains why tracking silicon IP is so difficult. "If it is in a custom chip, the only practical technique is to etch open the package and look for it using a microscope. Even this technique is difficult for soft IP, which is processed by synthesis or automatic place and route tools. If the IP is on an fpga, then it is theoretically possible to use watermarking on the bitstream to detect IP. However, this technique is defeated if the person misusing the IP encrypts the bitstream."

Algotronix is one company developing solutions to simplify IP tagging and detection, having developed a circuit technique for tagging complete fpga or ic designs or IP cores. The tags have been designed to be small and low power, so that multiple tags can be realistically be on a single chip, with a sensor placed on the package to detect the tags. The technology will be launched at the forthcoming Design Automation Conference in June.

Open sesame?

With so much IP changing hands, it may not always be practical to defend every IP transgression – indeed, it may be advantageous to be more open with IP.

Recounts Bill Seymour, head of Nokia's Intellectual Rights department: "In certain cases, you want to create a bigger market – you will want to make sure that everybody has access to the technology." In this case, essential IP is submitted to a standards committee and the developer agrees to abide by fair, reasonable and non discriminatory pricing when licensing the technology to other parties – including direct competitors.

Licensing revenues are just one way of obtaining value from IP, as a developer taking this route may also be able to negotiate cross licensing deals that provide access to other essential patents. The Open Source model is of course the ultimate extension of a freer approach to IPR, whereby a company forsakes its licensing rights in return for community R&D.

Inevitably, IP protection requires a multipronged approach. However, a balanced IPR strategy and open collaboration are now viewed as complimentary. Talking at a recent event about Nokia's ambition to be 'the best internet platform', Seymour affirmed that, whilst it would still protect its technologies: "Open collaboration and open standards … continue to be something that you hear from us. It was the key to success in gsm; it is the key to success in internet."

EVIDENCE 2

DesignTag demonstration at the 44th Design Automation Conference

Why it is included

Evidence of a public technology demonstration in 2007 and of the original Red Tag and Black Tag product concepts.

Algotronix to demonstrate its DesignTag Electronic IP labelling technology at the 44th DAC in San Diego

May 18, 2007 -- Algotronix Ltd., a supplier of cryptographic intellectual property, announced that it will demonstrate its unique, patented, DesignTag active labelling technology at the 44th Design Automation Conference, Booth 885.

DesignTag is a machine-readable product labelling technology which can be applied to FPGA designs, ICs and Intellectual Property cores. Based on cryptographic research into 'side channels' DesignTag is a small, low power, active digital circuit supplied as an IP core for inclusion in larger designs. The presence of DesignTags can be detected by a sensor placed in contact with the package of the chip which contains them. DesignTag communicates a unique tag to the sensor which can then be used to access information on the tagged product in a web-based database.

Two families of DesignTag products will be demonstrated. The low cost Red Tag product addresses product identification and version control. Red Tag is particularly useful for FPGA users because ink markings on FPGA packages identify the FPGA chip, not the user design within. Moreover, ink markings on the FPGA package cannot track in-the-field updates to the FPGA bitsream. The Black Tag product is a hardened version of DesignTag intended for covert IP tracking and detection of IP licence infringement. Multiple Black Tags can be added to a single chip and are only detectable by their owner. Black Tags can be added to designs by CAD software and used to detect commercial chips which have been created using educational or evaluation copies of software tools.

Since DesignTag directly identifies the chip within the package it can be used by semiconductor vendors and chip users to allow them to detect products which have been fraudulently mislabelled – for example by changing speed grade or temperature range or marking a low cost clone product as a 'brand name' alternative.

Tom Kean, Managing Director of Algotronix commented, "For almost 50 years the chip industry has relied on ink markings on chip packages for product identification. With its DesignTag technology Algotronix has brought labelling technology into the 21st century by providing a machine-readable electronic tag circuit embedded in the chip and linked to a web-based database providing rich information on the tagged product. Unlike simple ink markings on the chip package this technology is accessible to FPGA designers, CAD companies, IP core vendors and design services organisations – and will allow them to take proper credit for their contributions."

About Algotronix

Based in Edinburgh, Scotland Algotronix develops and licences a range of encryption and design security intellectual property to customers throughout the world.
See: **www.algotronix.com**

Write your message:

send

E-mail This Article Printer-Friendly Page

list: -1180165229.64 seconds
detail: 0.000412940979004 seconds
prov: 0.000607013702393 seconds
end_new

EVIDENCE 3

EE Times: wireless DesignTag for IP cores

Why it is included

Independent specialist coverage explaining through-package detection, multiple tags, database lookup and access control.

Also published as

• Wireless Net DesignLine - Algotronix offers Wireless DesignTag for IP Cores

CMP United Business Media
ONLINE EETIMES europe
Global news for the creators of technology

Algotronix offers wireless "design tag" for IP cores

Peter Clarke
(05/25/2007 8:59 AM EDT)
URL: http://www.eetimes.eu/uk/199702130

Algotronix Ltd. (Edinburgh, Scotland), a consultancy spun out of Xilinx in 1998, is offering DesignTag, an active digital circuit element that can be designed-in to ICs and FPGAs and detected through-package by an external scanner.

LONDON — Algotronix Ltd. (Edinburgh, Scotland), a consultancy spun out of Xilinx in 1998, is offering DesignTag, an active digital circuit element that can be designed-in to ICs and FPGAs and detected through-package by an external scanner.

The scanner detects the presence of tagged intellectual property within an operating integrated circuit, providing a mechanism to identify falsely labeled chips and supporting enforcement of IP core and CAD tool license agreements.

Single or multiple tags can be present in a single chip and the scanner can read the serial number of each tag and use a separate web-based database to find out about a tagged chip. Security mechanisms allow DesignTag users to control who can detect their tag or to restrict elements of the information stored in the web database.

According to Algotronix the use of wirelessly readable tags would allow providers of IP cores to increase recognition for their work and increase the value of their cores and businesses. At present chip labeling is done in ink at the final stages of manufacture and recognizes the IDM that physically makes the system-chip (SOC) or the maker of the FPGA, but not the IP contributors.

"Sometimes, even the IC supplier goes without credit as powerful customers insist on marking key chips with their own logo. FPGA chip packages are marked by the FPGA vendors not the creators of the circuit they implement," Algotronix states in a brochure produced to promote DesignTag.

Algotronix is also offering DesignTag as a way to transcend other inherent problems in human-readable ink marking of chip packages, such as fraudulent marking, faded marking, lack of space and the fact that FPGAs can change their contents and function in the field.

The Algotronix' "Red Tag" product is intended primarily for product identification and version control. The "Black Tag" is a hardened version of the DesignTag intended for covert use and detection of intellectual property misuse. Multiple Black tags can be associated with a single chip.

The tag is digital and requires no special analog components, Algotronix said. Already small and low power the tag can be configured to switch off a few minutes after the chip is powered on, to save additional power. The sensor is an off-the-shelf component and data can be collected using a digital multimeter with datalogging capability or, more conveniently, using a data logging unit supplied by Algotronix which connects directly to a computer running the Algotronix software via a USB cable.

Algotronix is developing a web database that integrates the tag scanning software to deliver additional information on tagged products.

Customers will have the option to associate datasheets or marketing materials with tagged chips or to provide background information on the design. Alternatively such information can be withheld to keep the design information private and secret.

DesignTag is due to be demonstrated at the Design Automation Conference in San Diego on booth 885.

Related articles:

Algotronix ships G2 release of AES core Crypto IP company appoints Chinese distributor

RFID industry ratifies data-sharing standard

EVIDENCE 4

Commercial launch of the DesignTag system

Why it is included

Evidence that the technology progressed from demonstration to customer release, with reader hardware/software, technical resource figures, pricing and defined application markets.

Also published as

• SOCcentral - Algotronix Launches DesignTag

Algotronix launches unique DesignTag system for detecting proprietary intellectual property within an operating chip

May 19, 2008 -- Algotronix Ltd., a supplier of cryptographic intellectual property, announced that its unique DesignTag thermal active tagging system for identifying design intellectual property will be released to customers on 26th May. A technical paper on the technology will be presented at the Hardware Oriented Security and Trust workshop which is co-located with DAC.

DesignTag consists of a small, low power, IP core which is added to the design to be protected and DesignTag reader software and data logging hardware which can sense the tag through the chip package. Each DesignTag IP core has a unique identification code which can be used to look up details of the protected product in a database. The DesignTag IP core is a purely digital circuit which works by creating minute temperature changes which are then detected using a low cost thermocouple placed in contact with the chip package. The DesignTag reader software accesses a database of tag information and based on this demodulates the spread spectrum thermal signal transmitted by the tag and determines which tag is inside the chip. It then provides design information corresponding to that tag. Customers can decide whether to make their tag information available in the public database so that all users of the DesignTag reader can detect their tags or whether to keep their tags private for internal use only.

The first application area to be addressed is identifying the bitstream configured into FPGA chips; future products will address identifying intellectual property cores within SoC chips and detecting 'fake' integrated circuits in the supply chain where the package markings do not correctly identify the chip within. FPGA users are a natural market for DesignTag since the ink markings on an FPGA chip identify the FPGA manufacturer and model, not the user design configured into it.

In a typical application the DesignTag will consume around 5mW when active and will only be enabled for around 15 minutes after the protected chip is powered on. The energy costs are therefore negligible in most cases. The tag also requires very low silicon resources – around 200 slices on a Xilinx Spartan 3. Introductory pricing to use the DesignTag IP core in one FPGA design is £100 ($200) and the DesignTag reader software is priced at £400 ($800). Products and pricing to use DesignTag on ASIC and ASSP chips will be announced at a later date. The FPGA products are available from Algotronix' web store at **www.design-tag.com** . A data-logger such as the Pico Technology TC08 is also required to collect the temperature samples from the tagged chip.

DesignTag has the ability to transmit status codes under the control of the user's design – for example if the user design detects a fault condition it could instruct DesignTag to transmit a different code than it would use during normal operation. This can be a useful way of communicating fault information for diagnostic purposes in an embedded system where there is no other fault reporting mechanism.

Tom Kean, Managing Director of Algotronix commented, "Unlike simple ink markings on the chip package DesignTag is accessible to FPGA designers, CAD companies and IP core vendors and is secured against falsification. In an environment where blatant copies of all types of electronic equipment from cellular phones to complex medical electronics are being offered tagging an FPGA bitstream before letting it out of the building is simple common sense."

About Algotronix
Based in Edinburgh, Scotland Algotronix develops and licences a range of encryption and design security intellectual property to customers throughout the world.
See: **www.algotronix.com**

REQUEST OF INFORMATION

Contact Algotronix Ltd.

Fill out this form for contacting a *Algotronix Ltd.* representative.

Your Name:

Your E-mail address:

Your Company address:

Your Phone Number:

Write your message:

send

E-mail This Article Printer-Friendly Page

list: -1220900522.95 seconds
detail: 0.000248908996582 seconds
prov: 0.000337839126587 seconds
end_new

Home | **Feedback** | **Register** | **Site Map**

CMP
United Business Media

EVIDENCE 5

FPGA Journal: DesignTag system and product positioning

Why it is included

Specialist FPGA coverage of the thermal signature, watermarking proposition, Red and Black variants, licence pricing and starter kit.

techfocusmedia
FPGA and Structured ASIC JOURNAL
TRENDS
TECHNOLOGY
TOOLS
TECHNIQUES

Source: Algotronix
July 21, 2008

Algotronix Introduces DesignTag System

Wednesday, 9 July 2008

Algotronix Ltd., Edinburgh, UK has launched a novel concept in tagging to help counter the rapidly growing trade in stolen IP, counterfeit chips and cloned designs. The financial cost to the industry of fake components and IP theft has been estimated at $2B to $3B.

DesignTagTM is a small low-cost IP core that can be included into an FPGA design or built into a semiconductor. It allows ownership of the design to be positively established and helps in the fight against piracy and fraud.

DesignTag is a digital core coded with a customer-specific 'signature' that can be identified externally from a working device without needing to read the FPGA bit stream or decapsulate the chip. It works by modulating the power dissipation of the host device by around 5mW which creates small temperature changes which are sensed by a thermocouple and decrypted by the reader software running on a PC. Ownership details are then simply extracted from the database. Algotronix has leveraged its skill base in crypto products to create a highly secure method of 'watermarking' designs.

With the rise of programmable logic it is now easier than ever to steal a design by copying the configuration bit stream. "The problem is how to deter theft and prove ownership of the design," said Tom Kean, Managing Director of Algotronix. "This is where DesignTag can help. The circuitry for DesignTag will be buried inside the FPGA bit stream and very difficult to locate and disable – even if the fraudster knows that it is included".

The tag can also be used to confirm the design revision loaded into the FPGA or to signal internal status conditions, such as, when an overflow has occurred or a soft error was detected in memory. Signalling is done without interrupting the system operation or accessing package pins.

The DesignTag version shipping today for use with FPGAs is called DesignTag Red. This is available at an introductory price of $200 per code license. DesignTag Reader Software is available separately at a cost of $800, and a Starter Kit comprising an Evaluation Board and thermocouple data logger, together with the Reader Software and licenses for five codes is shipping at $2,000. An ASIC/ASSP version of DesignTag will also be available; this is targeted at identifying rebranded semiconductors and will form a key mechanism to uncover parts that have been fraudulently remarked to enhance their value.

DesignTag Red is included into the top level design to protect the company property. A different version to cover the license enforcement needs of third party IP core and CAD tool suppliers will follow shortly and is designated DesignTag Black. It also provides a mechanism for IP core vendors to obtain product version or status information from IP cores embedded in a larger design. In this application the top level designer is prevented from disabling or removing the tag by additional protection mechanisms.

For more information: http://www.algotronix-store.com

EVIDENCE 6

EE Times: thermal signalling added to DesignTag

Why it is included

Detailed reporting of the working principle, the roughly 5 mW thermal modulation, the FPGA product and planned ASIC/ASSP application.

Also published as

- Automotive DesignLine - Algotronix Adds Thermal Signaling
- EE Times Asia - DesignTag Digital Core Adds Thermal Signaling
- ECNMag - IP Core Watermark Technology Protects Chip Designs
- New Electronics - Put a Tag on It

CMP United Business Media
EE Times

Algotronix adds thermal signaling to IP core DesignTag

Peter Clarke
(07/18/2008 7:05 AM EDT)
URL: http://www.eetimes.com/showArticle.jhtml?articleID=209101027

LONDON — Algotronix Ltd. (Edinburgh, Scotland), has added 'thermal signaling' to DesignTag, an active digital circuit element that can be designed-in to ICs and FPGAs and detected through-package by an external scanner.

Algotronix, a consultancy spun out of Xilinx in 1998, has been offering DesignTag for over a year. DesignTag is intended to provide a method of identifying falsely labeled chips and supporting enforcement of IP core and CAD tool license agreements.

DesignTag is a digital core coded with a customer-specific signature that can be identified externally from a working device without needing to read the FPGA bit stream or take the chip out of its package. It works by modulating the power dissipation of the host device by around 5mW which creates small temperature changes which are sensed by a thermocouple and decrypted by the reader software running on a PC.

Single or multiple tags can be present in a single chip and the scanner can read the serial number of each tag and use a separate web-based database to find out about a tagged chip. Security mechanisms allow DesignTag users to control who can detect their tag or to restrict elements of the information stored in the web database.

According to Algotronix the use of wirelessly readable tags would allow providers of IP cores to increase recognition for their work and increase the value of their cores and businesses. At present chip labeling is done in ink at the final stages of manufacture and recognizes the IDM that physically makes the system-chip (SOC) or the maker of the FPGA, but not the IP contributors.

The problem is how to deter theft and prove ownership of the design, said Tom Kean, managing director of Algotronix, in a statement.

The tag can also be used to confirm the design revision loaded into the FPGA or to signal internal status conditions, such as, when an overflow has occurred or a soft error was detected in memory. Signaling is done without interrupting the system operation or accessing package pins.

The DesignTag version shipping today for use with FPGAs is called DesignTag Red. This is available at an introductory price of $200 per code license. The DesignTag reader software is available separately at a cost of $800, and a starter kit comprising an evaluation board and thermocouple data logger, together with the reader software and licenses for five codes is shipping at $2,000. An ASIC/ASSP version of DesignTag will also be available; this is targeted at identifying rebranded semiconductors and will form a key mechanism to uncover parts that have been fraudulently remarked to enhance their value.

DesignTag Black is a version to cover the license enforcement needs of third-party IP core and CAD tool suppliers. It also provides a mechanism for IP core vendors to obtain product version or status information from IP cores embedded in a larger design. In this application the top level designer is prevented from disabling or removing the tag by additional protection mechanisms.

Thermal signaling

Thermal signaling works by modulating the power dissipation of the host device in a predefined way. Heat pulses propagate through the chip package with low attenuation. The level of the power surge is selected to provide a package temperature rise of around 0.1 degrees C. The additional dissipation is typically 5mW, against an operational power consumption of greater than 150mW for a mid-sized Xilinx Spartan FPGA.

The DesignTag defaults to turn off after 15 minutes of operation. This has two effects. Firstly it eliminates the small incremental power consumption, and secondly it also makes detection by a fraudster more difficult as power has to be cycled.

The thermal output by the DesignTag takes the form of a 64-bit code. A spreading code is used to control the heat generator using a circuit similar to a linear feedback shift register. The spreading-code generation circuit is based on the 'Tag ID' which acts like a cryptographic key, where each key results in a different pseudo-noise sequence.

The use of thermal signaling has several advantages over RF signaling in environments where electromagnetic interference is being suppressed, Algotronix claims. However, the technology is not recommended for chips used with heatsinks or with forced-air cooling.

Related articles:

How will encrypted chipmarking moves impact tear-downs?

Crypto IP company appoints Chinese distributor

RFID industry ratifies data-sharing standard

EVIDENCE 7

When the chips are down: beating the counterfeiters

Why it is included

A distinct product-oriented article framing DesignTag against counterfeit chips, cloned designs and IP theft.

Enquire for further information

When the chips are down: beating the counterfeiters

28 August 2008

The financial cost to the industry of fake components and IP theft has been estimated at $2 to $3bn. Among various systems available to counter this criminal practice is a novel concept for chip tagging developed by an Edinburgh based company

Edinburgh based Algotronix has launched a novel concept in tagging to help counter the rapidly growing trade in stolen IP, counterfeit chips and cloned designs. DesignTag is a small, low-cost IP core that can be included in an FPGA design or built into a semiconductor. It allows ownership of the design to be positively established and helps in the fight against piracy and fraud.

The system comprises a digital core coded with a customer-specific 'signature' that can be identified externally from a working device without having to read the FPGA bit stream or de-encapsulate the chip. It works by modulating the power dissipation of the host device by around 5mW; this creates small temperature changes which are sensed by a thermocouple and decrypted by the reader software running on a PC. Ownership details are then simply extracted from the database.

With the rise of programmable logic it is now easier than ever to steal a design by copying the configuration bit stream. "The problem is how to deter theft and prove ownership of the design," says Algotronix managing director, Tom Kean. "This is where DesignTag can help. The circuitry for DesignTag is buried withing the FPGA bit stream and is very difficult to locate and disable – even if the fraudster knows that it is included".

The tag can also be used to confirm the design revision loaded into the FPGA or to signal internal status conditions, such as, when an overflow has occurred or a soft error was detected in memory. Signalling is achieved without interrupting the system operation and without having to access the package pins.

The version shipping today for use with FPGAs is called DesignTag Red, currently available at an introductory price of $200 per code license. DesignTag Reader Software is available separately at a cost of $800, and a starter kit - comprising an evaluation board and thermocouple data logger, together with the Reader Software and licenses for five codes - is shipping at $2,000. An ASIC/ASSP version of DesignTag will be available shortly; this is targeted at identifying re-branded semiconductors and will be able to uncover parts that have been fraudulently remarked to enhance their value.

DesignTag Red is included in the top-level design. A different version, covering the license enforcement needs of third party IP core and CAD tool suppliers, will follow shortly and is designated DesignTag Black. It also provides a mechanism for IP core vendors to obtain product version or status information from IP cores embedded in a larger design. In this application, the top-level designer is prevented from disabling or removing the tag by additional protection mechanisms.

Contact Details and Archive...

- Algotronix Ltd

Related Articles...

- Data matrix code reading in the harshest environments
- Wi-Fi enabled Squirrel portable data logger
- Illegible bar codes no longer a problem
- Direct part marking guide
- HDD Technology for industrial and automated applications

Most Viewed Articles...

- Low-carbon transport
- Miniature disc couplings
- Mixed-signal oscilloscope family
- New standard in HVAC drives
- New Z Corp machine pulls the crowds at TCT2008

<< Back to Electrical & Electronic search results

EVIDENCE 8

How to defend against the cloning of FPGA designs

Why it is included

The most substantial technical article in the archive. It explains the threat model, proof-of-theft concept, implementation cost, detection method and applications in detail.

Also published as

• Digital Home DesignLine - How to Defend Against the Cloning of your FPGA Designs

September 17, 2008

How to defend against the cloning of your FPGA designs

Having your design cloned by a competitor isn't fun, so this "How To" design article explains how to foil your nefarious foes!

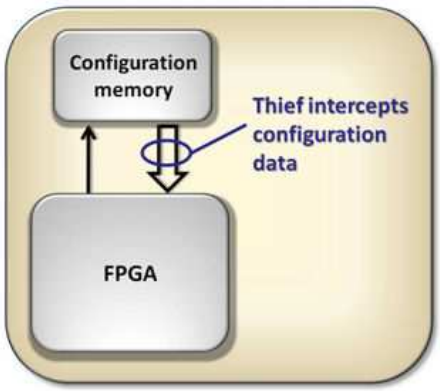
By Paul Dillien, High Tech Marketing

Editor's Note: *The technique described in this article is actually rather clever. May I suggest that, after reading the first section, you pause for a moment and try to guess how the DesignTag concept described below might be implemented. I bet that when you move on to the* "So how does it work?" *section you'll say to yourself (as I did):* "Wow, I would never have thought of that!"

This article describes a new way of tagging designs to help to counter the rapidly growing trade in stolen IP and cloned designs. The topic is a difficult one for the industry to discuss; recently, however, more and more voices have been raised on the issue.

An estimate of the prevalence of counterfeit electronics has been put as high as 10%. (The International Chamber of Commerce website, for example, includes the statement: *"Counterfeit electronics are estimated to account for 1 to 10 % of global electronic sales"*). This is supported by the Alliance for Gray Markets and Counterfeit Abatement (AGMA) (www.agmaglobal.org), an industry group that consists of Hewlett Packard, Cisco, and other top tier electronics OEM companies, which estimates the loss to manufacturers at more than $100B. The hidden costs of damaged reputations and reliability issues for the end customer are more difficult to quantify.

One unfortunate consequence of the rise of programmable logic coupled with the decline of the ASIC is that it is now easier than ever to copy a design. Some Asian or Eastern European companies openly claim to specialise in "reverse engineering" or copying PCB layouts and memory contents. It is difficult, expensive, and time consuming to reverse engineer an ASIC, but simple to copy the configuration bit stream of the most popular FPGAs (see *note) as illustrated in *Fig 1*.



1. Stealing an FPGA design is not complex.

***Note:** It is possible to encrypt bit streams for some SRAM based FPGAs. However, the overwhelming majority of customers do not use this because of added cost, complexity and logistics. The feature is not offered in the low cost parts that most customers use for high volume applications. Non-volatile FPGAs avoid this, but comprise only a small fraction of the overall market.*

As a result, companies can find that overnight their Intellectual Property (IP) appears in the product of a competitor. The counterfeiter carries virtually no R&D cost, and can therefore undercut the legitimate supplier on price and steal market share.

The problem is how to deter theft and prove ownership of the design. This is where a product called DesignTag from Algotronix can help. When buried in the FPGA bit-stream, the DesignTag code is very difficult to locate and disable – even if the fraudster knows that it is included.

Once this code is duplicated into the pirated bit-stream, it acts like a beacon announcing that the design has been copied. There is a strong parallel with the concept of marking valuables with your Post Code or Zip code using UV pens. It cannot prevent the theft, but allows ownership to be established afterwards.

2. DesignTag provides "proof-of-theft".

The DesignTag occupies $0.57 cents worth of silicon in a XC3S2000 FPGA (using the 100+ list pricing), which represents 1.3% of the logic resources on the chip. This is a modest overhead compared to the potential damage represented by illegal copies.

A more insidious problem comes from so called "over-building". The background to this problem lies in the mass exodus over the last decade of companies exiting production in favour of designing products to be built by contract manufacturers (CEM). This positions the CEM in a central and critical role. The vast majority of CEMs, of course, are responsible and provide a valuable service. Unscrupulous ones, however, can supplement their profits by producing more units than they are contracted for and selling the excess onto the gray market. Again the DesignTag identifies the source and ownership of the design.

A further application of DesignTag is to provide serial numbering or version identification. For example, medical, automotive, industrial, military, or aerospace manufacturers may wish to tag equipment with end customer codes or track the FPGA configuration version. Version control is especially important where upgrades are routinely applied. The DesignTag can be detected in working systems without making electrical contact and is particularly beneficial for ball grid arrays where the top of the package is far more accessible than the electrical connections. Monitoring can also be achieved without resorting to software or hardware interrupts that might affect the normal operation.

Yet another twist is to have an embedded system interact with DesignTag so that it flags fault or status conditions. In this application, the DesignTag is programmed to output a different code that unobtrusively signals the internal condition.

So how does it work?
This is really going to surprise you... go to page 2 of this article for all to be revealed...

So how does it work?
DesignTag is a small low-cost IP core that can be included into an FPGA as part of the design. It is a digital core with a unique code ("signature") that can be identified externally without needing to read the FPGA bit stream or internal registers.

It works by modulating the power dissipation of the host device in a predefined way. Tiny heat pulses propagate through the chip package with low attenuation. The level of the power "surge" is selected to provide a package temperature rise of only about 0.1 degrees C. The additional dissipation is typically 5mW, against an operational power consumption of >150mW for a mid-sized Spartan FPGA, which means the signal is deep below the noise floor.

The DesignTag defaults to turn off after 15 minutes of operation (the user can modify this value). This has two effects. Firstly it eliminates the small incremental power consumption, and secondly it also makes detection by a fraudster more difficult as power has to be cycled. Optionally, DesignTag can be triggered by an internal event from within the FPGA. This could be an instruction to transmit the ID code or to indicate an internal status or error condition.

The DesignTag database
The code data for all DesignTags is held in a central data base. Customers can choose whether they wish to make their code "public" or "private". The advantage of a public listing is that all DesignTag Reader Software will be enabled to detect the code, thereby allowing customers, enforcement agencies, and contract manufacturers to confirm the validity of the device under test (DUT).

By comparison, private codes may be preferred when the customer does not wish any third-parties to be able to tell whether or not their product is tagged. In this case codes are distributed by the customer to trusted parties – only their reader software with these codes installed will be enabled to detect the corresponding tags.

Incorporating DesignTag into an FPGA
The IP core for use with FPGAs is instantiated into HDL code as a "black box" in either Verilog or VHDL. The deliverable includes the in-built code which will drive the thermal output, as well as I/O pins that are required by the circuit. The all-digital design has a small footprint, typically requiring only 256 slices in a Spartan 3 FPGA from Xilinx.

The core is only available as an encrypted EDIF netlist for security reasons. The IP includes several techniques to prevent "reverse engineering" as well as other schemes designed to mask it from being tampered with or detected.

The core is largely independent of the user design, so the impact on the design flow is minimal.

DesignTag takes an input clock in the range 2-to-250MHz to drive the timing. The clock should be derived from any available clock inside the system rather than being generated specifically for the tag IP core for two reasons. Primarily, of course, it is the lowest cost option, but also it confuses attempts to detect and disable the tag by making it appear to merge into the system.

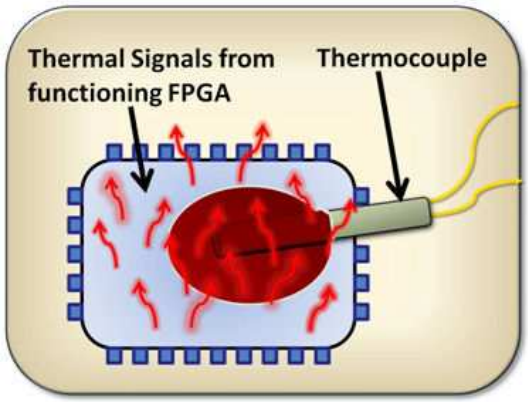
Control inputs for the DesignTag can be driven from the embedded system or set as defaults at the design stage. For example, the core can be set to transmit continuously if required; alternatively, the core can be instructed to transmit for a specified time on power-up, and to then enter a stand-by mode. As yet another option, the transmit sequence can be initiated at any time by a *Trigger* input.

The core is licensed with up to four different in-built codes, which are selected by the *Code Select* inputs. The embedded system can program the core to transmit one of these codes on command to indicate internal status conditions. For example, conditions indicating that an overflow has occurred or a soft error was detected in memory can be signalled without interrupting the system functionality.

A *Tamper Output* can be taken from the DesignTag into the embedded system. This has two benefits. It can be used as a disable signal that impairs the system performance and confuses an attempt to disable the tag by flipping random bits in the configuration bit stream. The second benefit is that if an attacker reverse engineers the bit stream to reconstitute the design, then the DesignTag block will appear as an integral part of the design.

Detecting DesignTag outputs

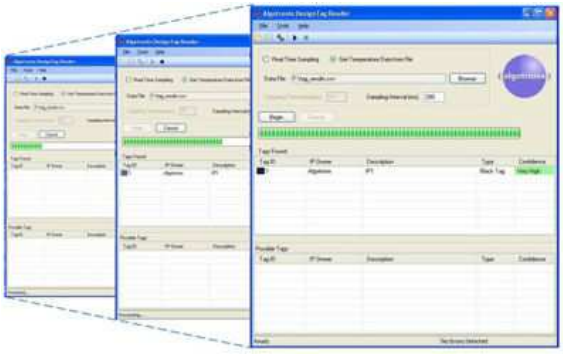
DesignTag codes are detected by placing a thermocouple in good thermal contact with the top of the package while the device is in operation as illustrated in *Fig 3*.



3. Detecting thermal signals with a thermocouple.

The thermal readings are input into the DesignTag Reader Software, which decrypts the signals. Detection time for a positive recognition of a code is measured in minutes, and the system can detect and differentiate multiple tags within the same device.

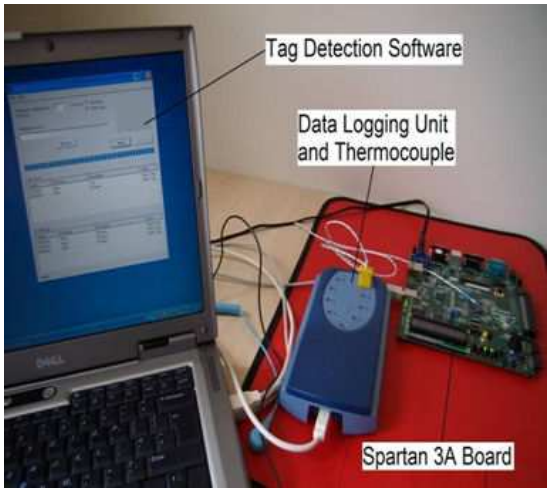
Poor conditions may increase the time required, but the underlying algorithms accumulate confidence with increased sample sizes (*Fig 4*). Acquisition time can be reduced if readings are taken in still air. The self-heating of the DUT as power is applied will not prevent the tag being detected. Factors that could increase the detection time include thermally erratic conditions, poor contact between the probe and the package or multiple codes in a single design.



4. The signals are accumulated and processed until a high confidence is achieved.
(Click this image to view a larger, more detailed version)

The DesignTag works with all popular styles of packages. However DesignTag is not recommended, at this time, for use with heatsinks or where forced air cooling is employed.

Algotronix recommends the TC-08 data logger with thermocouple from Pico Technology. Further devices are being evaluated. A TC-08 is included as part of the DesignTag Starter Kit along with the Reader Software, an evaluation board equipped with an FPGA and five active DesignTag codes (*Fig 5*). The Reader Software runs on a PC under Windows (XP or Vista).



5. The Starter Kit includes the Data Logger, Software, Evaluation Board, and five unique codes. (Click this image to view a larger, more detailed version)

Attempting to defeat DesignTag

One of the most important features for any anti-counterfeiting scheme is the difficulty of identifying, removing, or disabling the identity tag. This article will not go into a detailed description of the in-built countermeasures against removal and reverse engineering for obvious reasons, but let's consider how a counterfeiter might approach the job of defeating DesignTag.

The first problem for a potential thief is to identify if the stolen code contains the DesignTag or not. The tiny thermal signals take the form of a 64-bit code and can only be detected by using DSP and decryption techniques. A spreading code is used to control the heat generator using a Linear Feedback Shift Register (LFSR) like circuit (see *note).

***Note:** *See also this* Three-part mini-series on LFSRs.

The spreading code generation circuit is based on the unique 'Tag ID', which acts like a cryptographic key, where each key results in a different pseudo-noise sequence. The DesignTag Reader Software will readily identify public codes, but without prior knowledge and authorisation, the software is not enabled to detect private codes, which will remain hidden.

Various aspects of the tag waveform are pseudo-random. The code is designed to frustrate attempts to decode the signals by repeated power cycling and correlating the observed signals.

Another possible attack is to obtain multiple DesignTag IP cores and compare them at the bit-stream or encrypted netlist level in order to see which specific resources have changed on the assumption that these will correspond to code bits. To frustrate this attack, many aspects of the tag IP core are varied in a random manner to create a very large numbers of differences between any two tag instances.

An attacker may try to disable the DesignTag. It is instantiated into an FPGA design as a black box at the design capture stage and once included is incorporated into the bit stream that configures the SRAM device. Users can choose to encrypt their bit stream, but most do not.

FPGA configuration bit streams typically range from 2 Mb for a mid-range Spartan device, through to 10's of Mb for the larger Virtex family. Fraudsters may attempt to use software to reconstruct a netlist from the bit-stream information.

While such software has been created in the past and has been reported in the technical literature it appears that such tools are not currently openly available to hackers. The output of such software would be a flat netlist of the design after mapping onto FPGA primitives; while this is a step forward from a bit-stream, it is still a long way from the original design source code.

The fraudster could also try and manipulate the design at the bit-stream level by selectively 'flipping' bits and monitoring the effect with a view to shutting off security features. This is a more practical attack since it does not depend on developing or acquiring bit-stream reverse engineering software. It does require recalculating the checksum on the FPGA bit-stream so it is not totally straightforward.

The key to defeating this attack is to make the time needed for each *'flip a bit and see what happens'* cycle as long as possible and to make it difficult for an attacker to determine whether the security features have in fact been completely disabled. The fact that it takes several minutes to read a DesignTag code makes search based attacks such as this less feasible.

An advantage of DesignTag compared with FPGA design security mechanisms such as Device DNA or challenge/response schemes which involve accessing an external chip through I/O pins is that DesignTag is not tied to specific resources on the FPGA which have easily determined locations in the bitstream.

FPGAs based on Flash or anti-fuse technology are configured in the factory and so the code containing the DesignTag is not exposed to the end user. Any attack on the DesignTag would involve physically tampering with the device and result in destroying the FPGA.

Why thermal and not electrical signals?

By this time you are probably wondering why an unconventional signalling medium was chosen.

The most obvious mechanism to signal to circuits within a chip is through package pins. However, there are important drawbacks to this mechanism in this context. To be useful to an end user, the tag mechanism has

to be independent of the circuit board onto which the chip has been designed and independent of any system software.

In some cases, the developer of the circuit board and system software may be the party suspected of misuse of the IP. Also, accessing the tag should not require detailed knowledge of the system containing the suspect chip. With BGA chips and fine pitch flat packs, even the act of finding an appropriate place on a circuit board to probe a signal can be quite tricky. Accessing tag information through package pins will generally require a trained technician.

The bandwidth of a thermal path through a package is low, and well-matched to the signalling scheme adopted for DesignTag. The data transmission rate is slow, but very few bits are needed to create the code and the thermal approach gives some additional advantages.

Thermal signals are transmitted through the package and detected by a probe in contact with the package top. No interruption to the normal operation of the device is required and no access is needed to electrical connections. No additional package pins are required either so DesignTag can be added to existing products without changing their pin-out.

Readings can be taken from a device in-situ or in a test jig by a semi-skilled operator. High pin count ball grid arrays require dense PCB traces, and it can be a problem to trace out additional tracks to test points and might indicate to an attacker the presence of DesignTag.

Signalling from the tag using EMI, RF or power supply noise is also theoretically possible. A low level electrical signalling scheme would suffer from extraneous noise from the activity on the chip, fast power supply glitches and ground bounce, as well as coupling from activity on nearby PCB traces. External sources such as radio waves, mains power sources, and other EMI also cause interference.

Modern systems require multiple power supplies that must be well screened and decoupled. The supply smoothing would be fighting against the attempted signalling back out from the chip, and might compromise both the chip performance and the quality of the tag signalling. Potentially, the wide bandwidth of electrical signalling offers a much faster detection, but experimentation showed that this was more than offset by the issues discussed above.

Summary

The cost of stolen IP and cloned designs is growing fast. The innovative DesignTag technology presented in this article provides a low-cost and easy way to add a watermark to your design. Tagging your design provides a simple way of proving piracy or fraud without resorting to lengthy engineering evaluation. Detection of counterfeit parts in minutes rather than days or weeks makes it a viable solution.

New applications are being dreamt up for DesignTag as more users come to appreciate its features. Time will tell which applications become the most popular for this patented product from Algotronix (Click Here for more information on DesignTag).

Paul Dillien *has worked in the semiconductor industry for over 30 years, including various Sales and Marketing roles at Xilinx, Plessey, and Ferranti. More recently, Paul founded the high-technology marketing consultancy company* High Tech Marketing*. Paul can be contacted at* paul@high-tech-marketing.co.uk.

EVIDENCE 9

Pico Technology newsletter

Why it is included

Supplier-side evidence that the DesignTag reader used a Pico Technology thermocouple data logger, showing integration with commercially available measurement hardware.

Pico
Technology

Pico Technology Test & Measurement Newsletter — October 2008

Here is your monthly Test and Measurement update.

1. TC-08 Thermocouple Data Logger in the News

If you're an FPGA designer, you might be interested in DesignTag, a new idea for protecting your IP. Developed by UK company Algotronix(http://www.algotronix-store.com/) , it uses a Pico Technology TC-08 Thermocouple Data Logger(http://www.picotech.com/thermocouple.html) .

What could possibly be the connection between IP protection and a thermocouple data logger?
Read this technical paper about DesignTag(http://www.design-reuse.com/articles/18755/protect-chip-designs.html) on the "Design Re-Use" site to find out.

2. New Technical Note: Channel Scaling with PicoScope 6

With four-channel scopes, you need to keep your traces organised to avoid confusion. Our latest technical note explains how to use channel scaling and offset to arrange multiple traces on the display, and to avoid a mistake made by many oscilloscope users that can cause you to lose measurement resolution. Read on and keep your PicoScope 6 skills up to date.

Read "Channel Scaling with PicoScope 6"(http://www.picotech.com/support/kb/kbfiles/PositioningMultipleTracesInPicoScope6.pdf) (982 kB PDF)

3. Get Even More for Your Money with the PT-104

The PT-104 is a four-channel temperature converter for platinum resistance thermometers (PRTs) that provides 0.01 °C accuracy, 0.001 °C resolution and a -200 °C to +800 °C temperature range. We are now supplying the PT-104 with a free USB-to-serial converter (MI069, list price £25) so that you can use it with any PC that has either an RS-232 or a USB port.

The PT-104 is supplied with our PicoLog data logging software, which is regularly updated. You can always download the latest version, free of charge, from our website.

4. New Range of Oscilloscope Probes

As our range of oscilloscopes keeps growing, so does our selection of scope probes. We now have a 500 MHz passive probe for high-bandwidth scopes, and a number of active differential probes.