KANSAS CITY NSC National Security Campus

PHYSICALLY UNCLONABLE FUNCTIONS USING INTRINSIC MATERIAL PROPERTIES OF SEMICONDUCTORS

Background

Detecting and preventing the use of counterfeit electronic devices is a major imperative for both consumer and defense electronics. One way to assure the authenticity of an electronic device is to incorporate a marker that is created while the integrated circuit (IC) is fabricated. The marker, or fingerprint, can be validated at any point in the supply chain, ensuring that the part was manufactured and handled in a trusted fashion. Current methods for IC validation utilize physically unclonable functions (PUFs). PUFs take advantage of small variations between each device that exist due to the manufacturing process. The variations are not controllable, and thus are impossible to replicate. While PUFs based on variations in electrical characteristics show promise, they suffer from temperature instability, complex circuit design, and lack of implementation in non-CMOS devices.

Description

A PUF based on variations in material properties, instead of electrical properties, overcomes the limitations of an electrical PUF, but maintains the ability to incorporate a unique fingerprint during the manufacturing process. One of the first processing steps in the wafer fabrication process is ion implantation. In this step, high energy ions bombard the surface, creating localized defects that are later recrystallized upon thermal annealing. One attribute of the recrystallized regions in silicon is that they can emit light when stimulated by a voltage or a light source such as a laser. As with all wafer manufacturing processes, there are small variations that occur during the implantation and annealing process, such as implant energy and dose, and anneal temperature. These variations in turn lead to variations in the light emitted, creating unique optical fingerprints for each chip. Ion implantation is common for non-Si CMOS devices, such as GaAs and GaN, making this optical fingerprint method applicable to other semiconductor platforms.

Advantages

The material PUF seeks to overcome the limitations of the common electrical PUF, while maintaining the ease of manufacturing by utilizing variations in standard wafer processing. The material PUF is a significantly simpler device than the current electrical PUFs, requiring minimal design or additional processing. In order for the implanted regions to emit light, a simple two-terminal device is all that is required to apply the operating voltage. In contrast, electrical PUFs are based on architectures such as ring oscillators or arbiters, entailing the design of complex integrated circuits. The material PUF also requires much less space on the chip, and could be implemented in unused space between circuits.

A second advantage is the ability to implement the material PFU in non Si-CMOS devices. For example, GaAs and GaN wafers can be implanted with ions, such as erbium and europium, which lead to changes in the light emission properties of the localized region. The ability to apply the material PUF concept to non-Si wafers is a significant benefit over the electrical PUF.

Honeywell

The Department of Energy's Kansas City National Security Campus is a multi-mission engineering, manufacturing and sourcing enterprise delivering trusted national security products and government services. Managed by Honeywell Federal Manufacturing & Technologies, LLC., for the DOE under contract number DE-NA0002839.

14520 Botts Road, Kansas City, MO 64147 | 816.488.2000 | August 2017

A third improvement of the material PUF is the temperature stability of the device. The electrical PUFs suffer from reliability and repeatability issues when subjected to temperatures over 150 C. This is because the CMOS circuits are not rated above this temperature. In contrast, the material PUF is only limited by the temperature stability of the electrical contacts to the implanted region. This makes the material PUF capable of stable and reliable operation under high temperatures and other harsh environments.

Applications

The primary application for the material PUF will be in the microelectronics supply chain, both for defense and commercial applications. For defense applications, it is a process that can be easily implemented at any wafer foundry, and creates a more secure and trusted supply chain for critical programs. It can also be implemented in commercial wafer foundries, reducing the threat of counterfeit components entering the marketplace.

- Ability to “finger print” a high volume commercially manufactured device, such as FPGAs, at the foundry, and track throughout the supply chain
- Secure supply chain for application specific integrated circuits and RF devices used in defense programs
- Implementation for high volume consumer products such as controllers for brakes and air bags, or commercial aviation

Intellectual Property Status

This technology is patent pending under US Patent application number 14/973,383 filed 12/17/2015.

Keyword List

Physically Unclonable Function (PUF), Anti-Counterfeit, Optical Fingerprint, Trusted ICs, Circuit Authentication

Contact

Andrew Myers
816-488-4432
amyers@kcp.com

Honeywell

The Department of Energy’s Kansas City National Security Campus is a multi-mission engineering, manufacturing and sourcing enterprise delivering trusted national security products and government services. Managed by Honeywell Federal Manufacturing & Technologies, LLC., for the DOE under contract number DE-NA0002839.

14520 Botts Road, Kansas City, MO 64147 | 816.488.2000 | August 2017