Synopsys and Intrinsic-ID Collaborate to Accelerate Implementation of Security for IoT Edge Devices

Integration of Intrinsic-ID PUF Solution and Synopsys ARC EM Processor with SecureShield Enables Implementation of Security Functions without Requiring Dedicated Security Processor

MOUNTAIN VIEW, Calif., Feb. 18, 2016 /PRNewswire/ --

Highlights:

- Synopsys' ARC EM Processor with SecureShield technology enables an ultra-low power, firmware-only implementation of Intrinsic-ID's Physically Unclonable Functions (PUF) without additional hardware
- Intrinsic-ID's PUF technology allows a unique device fingerprint to be extracted from embedded SRAM for user, device and data authentication, or to derive an unclonable cryptographic root key
- Synopsys' SecureShield technology provides a secure environment that enables application software to execute sensitive cryptographic operations with PUF-derived keys, without ever exposing the keys
- Demonstration at Mobile World Congress shows authenticated logging of sensor values to a cloud service with PUF technology running on an ARC EM Processor with SecureShield technology

Synopsys, Inc. (Nasdaq: SNPS) and Intrinsic-ID today announced the integration ofIntrinsic-ID's PUF technology with Synopsys' DesignWare® ARC® EM Processors with SecureShield™ technology to enable efficient implementation of security functions such as authentication and device cloning prevention for low-power Internet-of-Things (IoT) edge devices. Intrinsic ID's Quiddikey® product is a secure key management solution based on their PUF technology that dynamically reconstructs on-chip secret keys without ever storing them, while Synopsys SecureShield technology provides a secure environment isolated from user code to protect the unclonable key. This combined solution enables system-on-a-chip (SoC) developers to support security-sensitive transactions, such as smart payment and secure cloud storage, found in applications including wearables and smart home appliances, without the cost or power consumption of a separate security processor core. SoC developers can add a complete security stack to low-power microprocessors and sensors without modifying any hardware.

"The rapid proliferation of connected devices and the new business models built on them have made secure user, device authentication and the management of valuable data critical," said Pim Tuyls, CEO at Intrinsic-ID. "With the combination of Synopsys and Intrinsic-ID IP, designers can deploy a firmware-only implementation of our unique PUF technology in a trusted execution environment by leveraging Synopsys' ARC EM processors with SecureShield. This solution enables the creation of highly secure, low-power SoCs that deliver superior anti-tamper and anti-cloning features for a wide range of IoT applications."

Intrinsic-ID's PUF security technology, called Hardware Intrinsic Security™ (HIS), uses a device-unique authentication process to extract security keys and unique identifiers from the innate characteristics of the SRAM. This extraction is done with Intrinsic-ID's Quiddikey product. Quiddikey guarantees the entropy of the key as well as a correct and secure key reconstruction under all circumstances. The PUF key is extracted from the chip and not externally programmed or stored; it is linked to the chip's unique physical characteristics and inherently protected against cloning and tampering.

DesignWare ARC EM Processors are based on the scalable, 32-bit ARCv2 instruction set architecture (ISA) and are optimized for area and power efficiency, making them ideally suited for IoT edge devices. Synopsys' Enhanced Security Package with SecureShield technology provides the ability to encrypt instructions and data, enabling designers to create a tamper-resistant, secure environment that protects their systems and software from evolving security threats such as IP theft and remote attacks. Intrinsic-ID's PUF solution can be implemented in firmware leveraging a trusted execution environment provided by Synopsys' SecureShield, isolating critical security functions from the application software running on the ARC EM processor. The DesignWare CryptoPack option provides the ability to speed up software encryption implementations by adding custom instructions and registers to the ARC EM processors. This further accelerates the PUF and associated security algorithms to maximize performance and minimize power consumption when executing data authentication and encryption.

"As more personal data is being transmitted in connected systems and devices, consumers are becoming increasingly concerned about the privacy and security of their information," said John Koeter, vice president of marketing for IP and prototyping at Synopsys. "Our collaboration with Intrinsic-ID provides designers with an advanced security solution that enables them to combine Intrinsic ID's PUF solution and Synopsys' ARC EM Processors with SecureShield technology for a faster, easier path to securing their IoT devices with strong authentication and the prevention of copying, cloning and other malicious attacks."

Availability and Resources

Synopsys' Enhanced Security Package, including SecureShield technology and CryptoPack options for ARC EM processors are available now from Synopsys.

Intrinsic-ID's PUF solution is available now from Intrinsic-ID.

A demonstration of Intrinsic-ID's PUF technology operating on Synopsys' ARC EM Processor will be shown in the Synopsys suite, Hall 6, Stand 601MR at Mobile World Congress in Barcelona, Spain, February 22-25, 2016.

- Learn more about Synopsys' Enhanced Security Package for ARC EM Processors: https://www.synopsys.com/dw/ipdir.php?ds=em-enhanced-security
- Learn more about Synopsys' ARC CryptoPack option for ARC EM Processors: https://www.synopsys.com/dw/ipdir.php?ds=arc-security-options
- Learn more about Intrinsic-ID's PUF solution: https://www.intrinsic-id.com/technology/his/

About Intrinsic-ID

Intrinsic-ID is a world leader in the field of Cyber Physical Security Systems as a provider of "Physical Unclonable Functions" (PUF). Using patented PUF technology, secret keys and identifiers are reliably extracted from the physical properties of chips. Intrinsic-ID's wide range of security solutions serves the following markets: embedded systems, IoT, identification, automotive, communications, content distribution, pay TV, government and defense. www.intrinsic-id.com

About DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad DesignWare IP portfolio includes logic libraries, embedded memories, embedded test, analog IP, wired and wireless interface IP, security IP, embedded processors and subsystems. To accelerate prototyping, software development and integration of IP into SoCs, Synopsys' IP Accelerated initiative offers IP prototyping kits, IP software development kits and IP subsystems. Synopsys' extensive investment in IP quality, comprehensive technical support and robust IP development methodology enables designers to reduce integration risk and accelerate time-to-market. For more information on DesignWare IP, visit http://www.synopsys.com/designware.

About Synopsys

Synopsys, Inc. (Nasdaq:SNPS) is the Silicon to Software™ partner for innovative companies developing the electronic products and software applications we rely on every day. As the world's 16th largest software company, Synopsys has a long history of being a global leader in electronic design automation (EDA) and semiconductor IP and is also growing its leadership in software quality and security solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest quality and security, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com.

Editorial Contacts:
Monica Marmie
Synopsys, Inc.
650-584-2890
monical@synopsys.com

Boris Kennes
Intrinsic-ID, B.V.
+31 40 851 90 20
marketing@intrinsic-id.com

SOURCE Synopsys, Inc.