Synopsys Introduces Enhanced Security Package for DesignWare ARC EM Processors

New Option Enables Implementation of a Trusted Execution Environment on a Single, Ultra-Low Power ARC EM Core

MOUNTAIN VIEW, Calif., Nov. 4, 2015 /PRNewswire/ --

Highlights:

- New Enhanced Security Package option for ARC EM processors includes Synopsys SecureShield technology for development of a trusted execution environment
- In-line instruction and data encryption, address scrambling and data integrity checks provide protection from system attacks and IP theft
- Integrated watchdog timer detects system failures that result from tampering and supports countermeasures
- Ability to add secure custom instructions or coprocessors in a secure mode boosts performance and reduces power consumption

Synopsys, Inc. (Nasdaq:SNPS) today announced availability of the Enhanced Security Package, a new licensable option for DesignWare® ARC® EM Processors. This new ARC EM option enables designers to create an isolated, secure environment that protects their systems and software from evolving security threats such as IP theft and remote attacks. The Enhanced Security Package integrates Synopsys SecureShield™ technology, which provides support for separating secure and non-secure modes of operation and memory as part of a trusted execution environment. The new package also includes features such as instruction and data encryption as well as data integrity checks to defend against software attacks. The ARC EM Processor with Enhanced Security Package enables SoC developers to create devices less susceptible to security threats using a single, ultra-low power processor, which eliminates the increased area and power consumption that an additional security core and associated memories would entail. This combination of security features and energy savings is especially important for IoT and mobile applications, including wearables and smart home devices.

"As more sensitive data is proliferated throughout connected systems and devices, there is increasing concern about privacy and the security of embedded systems," said Pim Tuyls, CEO at Intrinsic-ID. "With its Enhanced Security Package, Synopsys is filling an important void in the industry by providing enhanced security features on a compact, ultra-low power core. Through our collaboration with Synopsys, IC developers using ARC EM Processors can easily create secure communication channels between devices with Intrinsic-ID's core PUF security technology."

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 a wide range of connected devices. The new Enhanced Security Package integrates SecureShield technology, which includes protected access control for the core functions and system bus and a secure memory protection unit (MPU) with up to 16 configurable memory regions. The secure MPU supports programmable permissions to enable or disable read, write, and execution of instructions and data to and from specific regions of memory; it also offers per-region scrambling or encryption. Combined with secure context switching, the configurable MPU enables multiple isolated execution contexts using a single core. In addition, programmers can use ARC Processor EXtension (APEX) technology to define custom instructions or coprocessor functions that can be restricted to execute only in secure mode, set at the time of the design or run-time programmable.

In addition, the ARC EM core's Enhanced Security Package includes an encrypted tamper-resistant pipeline and additional protection features to help prevent IP theft and system attacks. A combination of protected processor pipeline registers and in-line instruction and data encryption ensure decrypted instructions are never stored or accessible, protecting algorithms from reverse engineering without impact to the timing of instructions. The existing ARC EM error checking and correction (ECC) functionality has also been enhanced with data and instruction path integrity checking that triggers an exception when intentionally injected errors are detected. The Enhanced Security Package integrates a watchdog timer to detect and recover from tamper-related system failures.

The ARC EM Family is supported by a robust ecosystem of software and hardware development tools, including the ARC EM Starter Kit for early software development, MetaWare Development Toolkit that generates highly efficient code ideal for deeply embedded applications, ARC simulators including nSIM and xCAM, and the ARChitect core configuration tool. Synopsys' embARC Open Software Platform gives all ARC EM software developers online access to a comprehensive suite of free and open-source software that eases the development of code for IoT and other embedded applications.

"With the vast amount of personal data stored in the cloud and transferred between smart devices, effective security measures are needed to avoid the threat of data breaches and malicious attacks," said John Koeter, vice president of marketing for IP and prototyping at Synopsys. "By extending our portfolio of security solutions with Synopsys' new Enhanced Security Package for ARC EM cores, we are enabling designers to implement the necessary functionality into their secure connected devices without sacrificing performance, power and area required by the target application."

The Enhanced Security Package with SecureShield is a part of Synopsys' comprehensive portfolio of security IP solutions, which also includes the CryptoPack option for ARC EM processors as well as the DesignWare Security IP solutions, which comprise a range of cryptography cores and software, protocol accelerators, root of trust, platform security and content protection IP.

Availability and Resources
The Enhanced Security Package option is scheduled for general availability in December, 2015, for ARC EM4 and ARC EM5D processors; availability for additional ARC EM cores is planned for 2016.

- Learn more about the Synopsys' Enhanced Security Package for ARC EM Processors: https://www.synopsys.com/dw/ipdir.php?ds=em-enhanced-security
- Learn more about Synopsys' DesignWare Security IP Solutions: http://www.synopsys.com/IP/security-ip/Pages/default.aspx

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.

Forward-Looking Statements

This press release contains forward-looking statements within the meaning of Section 21E of the Securities Exchange Act of 1934, including statements regarding the expected release and benefits of the Enhanced Security Package for DesignWare ARC EM processors. Any statements that are not statements of historical fact may be deemed to be forward-looking statements. These statements involve known and unknown risks, uncertainties and other factors that could cause actual results, time frames or achievements to differ materially from those expressed or implied in the forward-looking statements. Other risks and uncertainties that may apply are set forth in the "Risk Factors" section of Synopsys' most recently filed Quarterly Report on Form 10-Q. Synopsys undertakes no obligation to update publicly any forward-looking statements, or to update the reasons actual results could differ materially from those anticipated in these forward-looking statements, even if new information becomes available in the future.

Editorial Contact:

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

SOURCE Synopsys, Inc.