Synopsys' New ARC Secure IP Subsystem Addresses Security Threats in Embedded SIM and Other High-Value Embedded Applications

DesignWare ARC Secure IP Subsystem Provides Programmable Hardware Root of Trust to Protect Against Malware, Tampering and Exploitation of Communication Protocols in SoCs

MOUNTAIN VIEW, Calif., Sept. 19, 2017 /PRNewswire/ --

Highlights:

- Pre-verified DesignWare ARC Secure IP Subsystem provides a trusted hardware and software SoC environment that protects against malicious attacks targeting mobile, IoT and automotive applications
- Integrated, ultra-low power ARC SEM Security Processor with SecureShield technology protects against side-channel attacks, theft of trade secrets and data breaches
- Hardware cryptography options accelerate encryption for a range of algorithms including AES, 3DES, SHA-256, RSA and ECC
- Secure instruction and data controllers provide external memory access protection and runtime tampering detection
- Subsystem software—including NIST-validated cryptography library, secure boot and SecureShield runtime library—leverages the subsystem's hardware features to provide a comprehensive security solution

Synopsys, Inc. (Nasdaq: SNPS) today announced the new DesignWare® ARC® Secure IP Subsystem, an integrated, pre-verified hardware and software IP solution that addresses increasing security threats in high-value embedded applications such as embedded SIMs (eSIMs), smart metering and embedded Universal Integrated Circuit Cards (eUICC). At the heart of the ARC Secure IP Subsystem is a DesignWare ARC SEM110 or SEM120D Security Processor with SecureShield™ technology, which enables the creation of a Trusted Execution Environment (TEE) with advanced security features to protect against side-channel attacks. The Secure IP Subsystem includes both software- and hardware-accelerated cryptography options as well as secure instruction and data memory controllers that provide confidentiality and authenticity for non-trusted memory accesses. The subsystem's hardware security features are complemented by software, including a NIST-validated cryptography library, SecureShield Runtime Library and secure boot support. By providing the integrated and configurable Secure IP Subsystem, Synopsys enables SoC designers to implement an area- and energy-efficient programmable root of trust (RoT) that protects high-value targets against malware, tampering and exploitation of communication protocols.

"Security is paramount throughout the complete IoT device lifecycle from secure element device manufacturing through enrollment, provisioning," said Mikhail Friedland, CEO at jNet ThingX Corporation. "The combination of Synopsys' pre-verified ARC Secure Subsystem with an implementation of our JavaCard OS facilitates certification of Common Criteria CC EAL5+ systems, providing customers a complete, secure solution that protects against malicious attacks."

Secure, Ultra-Low Power and Area-Efficient Processors

The DesignWare ARC Secure IP Subsystem offers the choice of ultra-low power ARC SEM Processors with SecureShield technology, which enables the creation of a TEE for secure code execution, secure handling of assets and tamper protection. The ARC SEM Processors offer advanced security features including side-channel protection, a tamper-resistant pipeline with inline instruction, data and address scrambling, error detection and parity checking on memories, and secure debug to protect against theft of keys, code or other sensitive information. With a single ARC SEM core, developers can create the hardware TEE, manage the SoC security perimeter and provide enough bandwidth to run additional embedded software, including applications requiring signal processing functions that are common in IoT edge devices.

Comprehensive Cryptography Software Library and Hardware Accelerators

The ARC Secure Subsystem offers cryptography options ranging from pure software implementations to dedicated hardware cryptography engines, providing SoC architects with the flexibility to balance the power, performance and area requirements for typical ciphers, hashes and MAC algorithms such as AES, DES/3DES, SHA-256, RSA and ECC. The ARC Secure Subsystem includes the NIST-verified DesignWare Cryptography Software Library, which implements widely used algorithms for a range of security functions including secure boot, secure communication and Transport Layer Security (TLS). The secure instruction and data controllers provide robust decryption of secure code and data with minimal latency overhead. The subsystem includes signing tools that assist designers in creating an encrypted code image, which is of particular importance when

the code is stored in non-secure external memory.

"The rapid proliferation of threats targeting IoT, automotive and industrial applications is requiring SoC designers to incorporate robust security starting at the architectural level," said John Koeter, vice president of marketing for IP at Synopsys. "By providing an integrated and validated secure IP subsystem, Synopsys enables developers to implement a highly secure, programmable root of trust that protects devices against complex threats such as malware and device tampering in high-value embedded targets such as eSIMs and secure elements."

Availability and Resources
The ARC Secure IP Subsystem is available now.

- Learn more about DesignWare ARC Subsystems
- Learn more about ARC SEM Processors and SecureShield technology
- Learn more about Synopsys DesignWare Security IP Solutions

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 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 15th 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 security and quality solutions. Whether you're a system-on-chip (SoC) designer creating advanced semiconductors, or a software developer writing applications that require the highest security and quality, Synopsys has the solutions needed to deliver innovative, high-quality, secure products. Learn more at www.synopsys.com/.

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

SOURCE Synopsys, Inc.