Synopsys' New High-Performance Secure Module with Cryptography Acceleration Speeds Security Functions by 100x

DesignWare tRoot H5 Hardware Secure Module with Root of Trust Provides Trusted Execution Environment for Unique Identity of SoCs

MOUNTAIN VIEW, Calif., March 20, 2017 /PRNewswire/ --

Highlights:

- DesignWare tRoot H5 Hardware Secure Module with Root of Trust protects sensitive information and data processing within an SoC
- Key management provides secure access to cryptographic keys and other on-chip secrets, extending trust throughout the system
- Multi-stage secure boot validates software and data integrity of the host CPU
- Secure remote device lifecycle management safeguards against evolving threats
- Secure instruction and data controllers protect access and detect runtime tampering in external memories

Synopsys, Inc. (Nasdaq: SNPS) today announced availability of its new high-performance DesignWare® tRoot H5 Hardware Secure Module (HSM) with Root of Trust, providing designers with a Trusted Execution Environment (TEE) that protects sensitive information and data processing within their system-on-chips (SoCs). The tRoot H5 HSM incorporates hardware cryptography acceleration to enable up to 100 times faster operation of security functions such as secure boot, secure updates and secure debug compared to software-only solutions. The complete, standalone product provides a secure hardware enclave with firmware components and tools, allowing designers to quickly integrate a security solution without requiring expertise to write security software. With the DesignWare tRoot H5 HSM, designers can easily create, store and manage secrets that are critical in industrial control, cellular communications and IoT hubs.

"As the range and targets of security attacks increase, integrating security features into our SoCs has become a critical part of the design process," said Stephen Oh, CEO at eWBM. "Synopsys' tRoot H5 HSM enables designers to accelerate the execution of cryptography operations for faster authentication and tamper detection in otherwise vulnerable applications."

"With the increasing liabilities that product manufacturers face, they require proven, ready-to-integrate IP to mitigate security risks," said Mats Nählinder, president and CFO of Riscure North America. "As a global security test lab and a market leader in security test, our business is to evaluate security solutions for their ability to protect against malicious attacks targeting hardware and software. Products with TEEs, such as the DesignWare tRoot H5 HSM, are becoming an industry-recommended approach to implementing robust, high-performance security functions in connected devices."

The DesignWare tRoot H5 HSM provides SoCs with a unique identity that cannot be tampered with, and extends the trust of that identity to other internal and external entities in the SoC. The tRoot H5 HSM provides security functions in a trusted environment as a companion to a host processor. The secure instruction and data controllers provide protected access and runtime tamper detection in external memories for code and data privacy protection without the added cost of additional dedicated secure memory. In addition, the controllers reduce system complexity and cost by allowing tRoot's firmware to reside in any non-secure memory space. The tRoot H5 HSM's ROM-less architecture can support system design changes at any time without risk of exposing the system memory to threats.

"As the number of secure interactions increases in connected devices, so does the need for SoCs to execute more functions in less time," said John Koeter, vice president of marketing for IP at Synopsys. "With the introduction of the tRoot H5 Hardware Secure Module, along with content protection IP, protocol accelerators and cryptography IP, Synopsys is addressing the requirements of highly secure systems to protect devices from evolving threats."

Availability and Resources

The DesignWare tRoot H5 Hardware Secure Module, part of Synopsys' portfolio of Root of Trust solutions, is available now.

- Website: DesignWare Root of Trust Solutions
- Webinar: Securing IoT Systems with a Root of Trust
- Datasheet: DesignWare tRoot Hardware Secure Modules

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

SOURCE Synopsys, Inc.

Additional assets available online: