Synopsys Accelerates FIPS 140-3 Certification with NIST-Validated True Random Number Generator IP

High-Quality DesignWare Security IP Protects Against Security Threats for Connected Devices

MOUNTAIN VIEW, Calif., June 4, 2020 /PRNewswire/ --

Highlights

- Standards-compliant DesignWare TRNG IP generates random numbers used to create cryptographic keys to protect data and operations
- Passing NIST CAVP demonstrates conformance to rigorous evaluation process and accelerates FIPS 140-3 certification for SoCs to meet or exceed the highest commercial and government standards
- Feature-rich IP is silicon-proven and easily portable across processes and technologies including the most advanced 5nm nodes

Synopsys, Inc. (Nasdaq: SNPS) today announced its DesignWare® True Random Number Generator (TRNG) IP has received validation by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm Validation Program (CAVP), paving the way for the lower-risk Federal Information Processing Standards (FIPS) 140-3 certification of customer end products. Synopsys' standards-compliant TRNG IP helps protect devices and their connections with other devices or the cloud. The TRNG IP provides high entropy random numbers that are essential for encryption, authentication, platform security and highly secure communication. Integrating DesignWare TRNG IP accelerates FIPS 140-3, Common Criteria, and other certifications, reducing design risk and time-to-market for connected IoT, automotive, and cloud communication system-on-chips (SoCs).

"With the increasing numbers and sophistication of threats to connected devices, ensuring security from the foundation of the SoC design is critical," said Saleel Awsare, senior vice president and general manager, IoT Division at Synaptics. "After evaluating multiple random number generator solutions, we selected the Synopsys DesignWare True Random Number Generator IP to protect our SoCs due to their proven, standards-compliant high-quality entropy and process portability."

True Random Number Generators are the basis of device security, as they create and protect sensitive information. Weak or predictable random numbers open the door for attacks that can compromise keys, intercept data, and ultimately hack devices and their communication. To help safeguard data quality, DesignWare TRNG IP meet international standards criteria developed to substantiate the truly random nature of TRNG IP in a verifiable and statistically rigorous manner.

Designing TRNGs that provide consistently high-quality entropy across process, temperature, voltage, and frequency variations is complex. Synopsys' certification-ready TRNG IP operates in a wide system clock dynamic range to support operating frequencies from 30MHz to 1+GHz as the system requires during different stages of operation. In addition, the TRNG supports virtualization to enable access to random numbers from multiple entities within the system concurrently in a secure manner.

"Hackers are expanding their targets to all areas where data is stored and transferred, from the cloud to the edge, making stringent security a requirement starting at the SoC level," said John Koeter, senior vice president of marketing and strategy for IP at Synopsys. "By providing comprehensive, silicon-proven security IP, Synopsys enables designers to create highly secure products that can defend against a wide range of attacks."

Availability & Resources

- DesignWare True Random Number Generator IP is available now.
- Read about True Random Number Generators for Heightened Security in Any SoC

About Synopsys DesignWare IP

Synopsys is a leading provider of high-quality, silicon-proven IP solutions for SoC designs. The broad Synopsys 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 Synopsys DesignWare IP, visit https://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 https://www.synopsys.com/.

Editorial Contacts:
Kelly James
Synopsys, Inc.
650-584-8972
kellyj@synopsys.com

SOURCE Synopsys, Inc.