Synopsys Announces Industry's First Security IP Solutions for New SHA-3 Cryptographic Hash Standard

Compliant DesignWare SHA-3 Cryptography IP Protects the Integrity of Electronic Content in Applications Including Message Authentication and Digital Signatures

MOUNTAIN VIEW, Calif., Sept. 29, 2015 /PRNewswire/ --

Highlights:

- DesignWare Cryptography IP solutions are compliant with SHA-3, the latest standard released by the National Institute of Standards and Technology
- IP solutions target a range of security applications such as message authentication, digital signatures, random number generation and key derivation functions
- The SHA-3 hash algorithm offers strong security with exceptional performance capabilities in hardware implementations and an advanced cryptographic hash scheme
- The DesignWare Security IP for SHA-3 is available as a standalone, configurable hash core, or as part of the cryptography software library or integrated in a security subsystem

Synopsys, Inc. (Nasdaq:SNPS) has announced the industry's first security IP solutions compliant to the Secure Hash Algorithm-3 (SHA-3) cryptographic standard from the National Institute of Standards and Technology (NIST). Synopsys' DesignWare® SHA-3 Cryptography IP solutions enable developers to protect the integrity of electronic information in applications such as message authentication and digital signatures, random number generation and key derivation functions. By providing security IP that is compliant to the SHA-3 standard, Synopsys enables developers to have the latest hash algorithm readily available for integration into their next-generation system-on-chips (SoCs).

Hash algorithms transform digital messages into a short message digest for use in digital signatures and other security applications. A change in the original message text creates a change in the digest, which makes it easier to detect modifications to the original message. The DesignWare SHA-3 Cryptography IP provides exceptional performance in specific hardware implementations compared to the prior generation SHA-2 algorithm. The SHA-3 IP is based on the Keccak hash scheme, which uses a new "sponge construction" domain extender that can be adjusted to trade security strength for higher throughput, generating larger or smaller hash outputs as needed. The DesignWare Cryptography IP solutions for SHA-3 do not replace the SHA-2 family of hash functions, which remains secure and viable, but instead provides chipset vendors and device manufacturers with an alternative solution to future-proof their devices.

"As it's increasingly important to secure devices against the growing number of data breaches and malicious attacks, IP providers need to stay ahead of the security standards," said John Koeter, vice president of marketing for IP and Prototyping at Synopsys. "Synopsys' DesignWare Security IP solutions for the new SHA-3 algorithm enable developers to incorporate the necessary IP early in their development process and protect devices against future security vulnerabilities."

Availability

The DesignWare SHA-3 Security IP is scheduled to be available in November 2015 as a standalone configurable hash core, as part of the cryptography software library or integrated in a security subsystem.

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 a leader in software quality and security testing with its Coverity® 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 DesignWare SHA-3 Cryptography IP security solutions. 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 Contacts:
Monica Marmie
Synopsys, Inc.
650-584-2890
monical@synopsys.com

Stephen Brennan
MCA, Inc.
650-968-8900, ext.114
sbrennan@mcapr.com

SOURCE Synopsys, Inc.