Synopsys Adds New Algorithms in DesignWare Security Protocol Accelerators to Increase Protection for IoT SoCs

Support for ChaCha20 and Poly1305 Encrypted Authentication Provides More Secure Alternatives for Internet Communications

MOUNTAIN VIEW, Calif., March 6, 2018 /PRNewswire/ --

Highlights

- DesignWare Security Protocol Accelerators offer a complete range of standards-compliant symmetric and hash cryptographic algorithms to protect SoCs from IoT attacks
- Supports up to 6.8 Gbps Poly1305, 4.5 Gbps ChaCha20, and 4.1 Gbps encrypted authentication at 500 MHz for efficient secure IoT connections
- Secure key access, Trusted Execution Environment support, and countermeasures against side-channel attacks increase protection against threats
- Highly configurable security IP enables designers to tune the implementation to their specific performance, power, and area requirements to meet the requirements of their target application

Synopsys, Inc. (Nasdaq:SNPS) today announced that it has added the ChaCha20 and Poly1305 (RFC7539) algorithms to its DesignWare® Multipurpose Security Protocol Accelerator IP, enabling designers to efficiently implement the latest encryption and authentication functionality to protect their IoT system-on-chips (SoCs). The Security Protocol Accelerator IP increases security protocol performance by supporting efficient data sequencing as well as parallel processing of cryptographic operations such as authentication and encryption/decryption. With the addition of these algorithms to the Security Protocol Accelerator IP, designers can secure Internet communication applications that rely on the Transport Layer Security (TLS) protocol version 1.2 and 1.3, including browsers, voice-over-IP devices, and smart home applications.

The DesignWare Multipurpose Security Protocol Accelerator IP accelerates a broad range of computationally intensive cryptographic algorithms as required by most security protocols, such as SSL/TLS, IPsec, WiFi and LTE. The Security Protocol Accelerator IP's advanced security features include Trusted Execution Environment (TEE) support, secure key access and differential power analysis countermeasures to increase protection against threats. The virtualization feature allows designers to share a single Security Protocol Accelerator instance across multiple host processors, or a multi-core processor, to offload security functionality for reduced gate count, small memory footprint, and simplified software management.

"SoC designers rely on security protocol accelerators to increase performance and reduce latency of cryptographic algorithms in SoCs," said John Koeter, vice president of marketing for IP at Synopsys. "The addition of the ChaCha20 and Poly1305 algorithms as well as side-channel countermeasures to the DesignWare Security Protocol Accelerator IP enables more secure Internet communication for millions of connected devices that rely on the TLS protocol."

Availability

The DesignWare Multipurpose Security Protocol Accelerator IP with support for Chacha20 and Poly1305 is available today. Support for the ChaCha20 and Poly1305 algorithms is also available in Synopsys' NIST-validated DesignWare Cryptography Software Library.

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 enable 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.