Security Protocol Accelerator

Highlights

- Highly customer configurable, silicon-proven security accelerators
- Support for cipher, hash and AEAD algorithms used in major security protocols using parallel hashing and encryption
- AES, DES/3DES
- SHA-3 hashing, HMAC, KMAC, cSHAKE, and XOF support
- ChaCha20 cipher, Poly1305 hash and combined AEAD algorithm
- Built-in scatter/gather DMA capability offloads the host processor
- QoS and virtualization features
- Secure Key Port to access confidential data stored in NVM
- Configurable AMBA® AXI™ and AHB™ system bus interfaces, with TrustZone™ support
- Optional
  - Wireless security algorithms ZUC, SNOW 3G and KASUMI
  - Chinese security algorithms SM3 and SM4
  - DPA/TA side channel countermeasures for AES, SM4, DES/3DES

Applications

- Networking protocols (e.g. TLS, IPsec)
- Wireless (3GPP, LTE, LTE-Advanced)
- Internet of Things (IoT)
- Mobile communications
- Automotive
- Content protection and digital rights management

Overview

Complex system-on-chip (SoC) requirements can include security at the MAC layer, VPN layer, and application layer. The DesignWare Security Protocol Accelerator (SPAcc) IP addresses these needs with support for the Wi-Fi, MACsec, IPsec, SSL/TLS/DTLS, and SRTP security standards. The SPAcc IP offers high throughput with support for mixed packet size traffic and low latency to preserve quality of service in voice and video applications in single- and multi-core processor architectures. The product is a highly customer configurable enabling solution to be tuned for specific applications providing differentiation in the market.

The DesignWare SPAcc optionally includes the following cryptographic support:

- 3GPP/LTE/LTE-Advanced wireless security: ZUC, SNOW 3G and KASUMI algorithms
- Chinese security: SM3 and SM4 algorithms
- DPA/TA side channel countermeasures: for AES, SM4, DES/3DES algorithms

DesignWare Security Protocol Accelerator

Most security protocols require computationally intensive confidentiality and authentication algorithms to be applied to the data. The DesignWare SPAcc IP provides a framework to apply the algorithms that include a programmable sequencer, secure DMA engine, and cryptographic/hashing resources that can handle a variety of protocols.

The SPAcc product reduces the system bus traffic and increases throughput by supporting efficient data sequencing as well as parallel processing of cryptographic operations (authentication and encryption/decryption).

The DesignWare SPAcc IP products support the following cryptographic modes and algorithms (ZUC, SNOW 3G, KASUMI, SM3, SM4 are optional add-on algorithms):

Cipher algorithms:

- AES, SM4, ChaCha20, DES, RC4, MULTI2, KASUMI, SNOW 3G-UEA2, ZUC 128-EIA3

Cipher modes:

- ECB, CBC, CTR, OFB, CFB, f8, XTS, UEA1, UEA2, 128-EEA1, 128-EEA2, 128-EEA3

Hash (MAC) algorithms:

- MD5/SHA-1
- SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)
- SHA-3 (SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE, cSHAKE, KMAC)
- HMAC
- SM3
- AES based MACs (XCBC, CMAC)
- SM4 based MACs (XCBC, CMAC)
- Poly1305
- KASUMI-f9, KASUMI-UIA1, SNOW 3G-UIA2, SNOW-3G-128-EIA1, AES-128-EIA2, ZUC 128-EIA3
- CRC-32-IEEE 802.3, Michael-MIC

Combined modes (AEAD modes):

- AES-GCM, AES-CCM, SM4-GCM, SM4-CCM, ChaCha20/Poly1305-AEAD

Multiple performance options are available for individual cipher and hash operations.

Cryptographic cipher and hash cores can also run in a different clock domain than the interface logic.

The Secure DMA (SDMA) gathers a packet distributed in memory for processing, then scatters the packet back to the same memory locations or contiguous memory if required. The SDMA operates on data descriptor tables (DDT) stored in host memory (Figure 1).

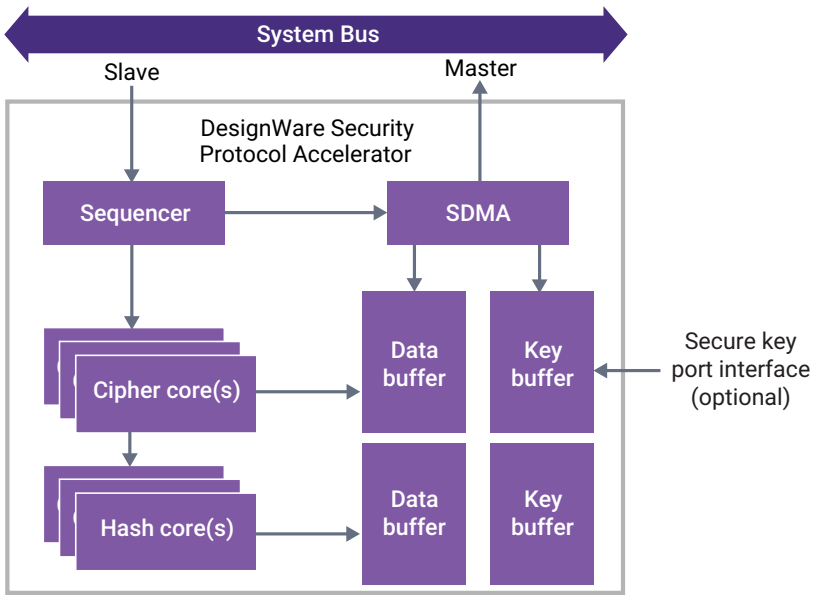

Figure 1: DesignWare Security Protocol Accelerator

QoS and Virtualization

The SPAcc offers unique QoS and virtualization features designed for high-performance SoC architectures (Figure 2).

QoS offers multiple priority queues used to support requirements such as latency optimization for voice and video traffic. Latency optimization allows traffic management applications to place the small, latency sensitive traffic into the high-priority queue and simultaneously manage larger packets through the low-priority queues to achieve the overall performance objectives.

Virtualization allows designers to share a single SPAcc engine across multiple processors, or a multi-core processor, to optimize security offload for significant gate count reduction and small memory footprint.

The SPAcc size and performance characteristics depend on the configuration selected. The size can range from 30K gates to 235K gates (or more), not including memories. At 350MHz, the AES-CBC-128 performance is 3 Gbps, the HMAC-SHA-1 performance is 1.7 Gbps, and the IPSec ESP AES-CBC-128- HMAC-SHA-1 transform performance is 1.7 Gbps.

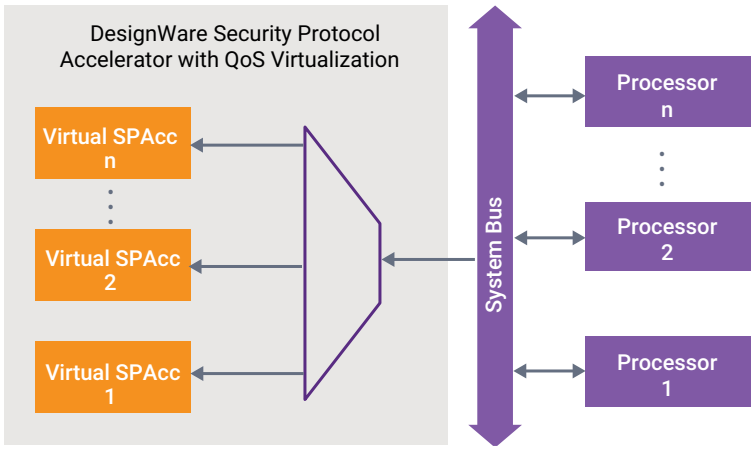

Figure 2: DesignWare Security Protocol Accelerator with QoS Virtualization

Deliverables

- Verilog HDL
- Testbench
- Sample synthesis script and constraints
- Sample simulation script
- Documentation

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 synopsys.com/designware.

SYNOPSYS®
Silicon to Software™

04/02/20.CS312298973_Security Protocol Accelerator _DS.