Public Key Accelerator

Highlights

- Offloads computationally intensive parts of public key cryptography
- Support for Arm® AMBA® AHB™/AXI™ and synchronous RAM slave interfaces
- Many build-time configuration options
- Configurable firmware memory type
  - RAM only
  - ROM only
  - RAM/ROM mix
- DesignWare cryptography software library for RSA, D-H, DSA
- DesignWare cryptography software library for prime field ECC operations such as ECDSA and ECDH
- SM2 Curve Support (Chinese Cryptography Curve)
- Optional: DPA/TA side channel countermeasures

Target Applications

- NSA Suite B
- IPsec and SSL gateways
- WiMax (IEEE 802.16) base stations
- Femtocells
- 3GPP/LTE
- Network processors
- E-commerce acceleration
- Military communications systems
- Payment card industry
- Secure manufacturing

Overview

Public key cryptography requires complex mathematical operations on very large numbers (from 160 to 4096 bits, or more). The majority of embedded CPUs are limited to operations on 32- and 64-bit values and require significant computational resources when implementing public key infrastructure related algorithms. The DesignWare® Public Key Accelerator (PKA) is dedicated to the computationally intensive elements of the mathematics required for RSA operations as well as the algorithms used in prime field elliptic curve cryptography (ECC). The PKA integrates seamlessly with the DesignWare cryptography software library, enabling designers to accelerate the asymmetric cryptography required in public key algorithms, to deliver performance levels that are not achievable in software-only solutions.

DesignWare Public Key Accelerator

The traditional RSA, digital signature algorithm (DSA), and Diffie-Hellman (DH) asymmetric algorithms require the calculation of complex modular exponentiation operations to encrypt, decrypt, sign, and verify data for public key negotiations or digital signature schemes. Similarly, ECC requires a number of complex mathematical operations, such as point multiplications, in support of public key negotiations and digital signature schemes.

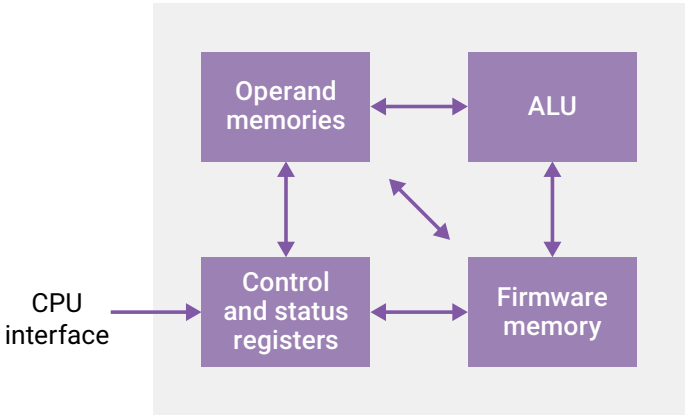

Figure 1: DesignWare Public Key Accelerator block diagram

Configuration	ASIC size K gate	Memory Bytes	RSA-1024 with CRT Ops/sec	RSA-2048 with CRT Ops/sec	ECC-160 Ops/sec	ECC-384 Ops/sec
32A	27	1280	187	N/A	323	N/A
32B	27	2560	187	32	323	60
64A	55	1280	381	N/A	408	N/A
64B	55	2560	381	92	408	116
128A	120	1280	605	N/A	470	N/A
128B	120	2560	605	195	470	169

- 40-nm at 340 MHz
- Firmware memory size not included
- RSA performance does not include pre-processing
- Full operand size, 50% hamming weight

Table 1: Typical Public Key Accelerator build options

The DesignWare PKA is designed to significantly accelerate these cumbersome operations. The highly configurable engine supports a broad range of mathematical operations, size, and performance options. These configuration options enable designers to select a wide range of capabilities suitable for applications ranging from base stations in WiMAX and 3GPP long term evolution (LTE) designs, to National Security Agency (NSA) Suite B and 10 Gbps security blades in network edge routers. Table 1 provides several data points for specific build options.

The DesignWare PKA is capable of executing the following integer and point operations:

- Integer operations (512-, 768-, 1024-, 1536-, 2048-, 3072-, and 4096-bit)
- Modular exponentiation - with and without Chinese Reminder Theorem (CRT)
- Modular division
- Modular multiplication
- Modular inversion
- Modular addition
- Modular subtraction

ECC-GF(p) operations (160-, 192-, 224-, 256-, 384-, 512- and 521-bit)

- Point multiplication
- Point addition
- Point double
- Point verification

These enhancements are useful for high security requirements such as FIPS-140, EAL (also known as common criteria used for banking) and payment card industry applications.

DesignWare Cryptography Software Library

The DesignWare Cryptography Software Library consists of widely used symmetric and asymmetric software algorithms that can be quickly rebuilt to support hardware acceleration for cryptographic operations and offload for embedded processors. The silicon-proven Cryptography Software Library has been rigorously verified through the NIST Cryptographic Algorithm Verification Program (CAVP). This library is available in source and binary formats.

Other Synopsys Security IP Cores

- DesignWare True Random Number Generator (TRNG) core
- DesignWare True Random Number Generator core for NIST SP 800-90c
- DesignWare Security Subsystems
- DesignWare Security Protocol Accelerator

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 enables designers to reduce integration risk and accelerate time-to-market.

For more information on DesignWare IP, visit synopsys.com/designware.

SYNOPSYS®
Silicon to Software™

03/27/20.CS12206_DesignWare Public Key Accelerator_DS.