SSL1-AXI Core

SSL/TLS Processor IP Core with an AXI Bus Interface

General Description

The SSL1 core implements SSL and/or TLS frameworks with a configurable variety of cipher suites.

SSL1-AXI has a “lookaside” interface to the rest of system through two AXI interfaces:

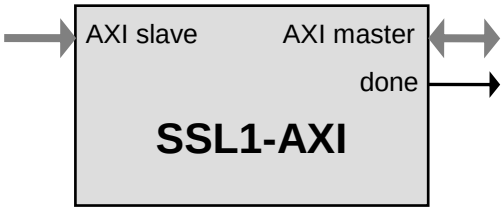
- AXI3/AXI4 slave for control
- AXI3/AXI4 master for data transfer

The data stream through the control interface contains processing commands. Each command consists a pointer to the descriptor in the system memory. Descriptor contains source, destination, encryption context, processing length, and status.

The encryption context (keys, encryption state, etc.) as well as the packets are stored in the system memory attached to the AXI bus and are read and written via the master interface.

The design is fully synchronous and is available in Verilog.

Symbol



Key Features

Throughput of 6-8 bits per clock (600-800 Mbps at 100 MHz)

Supports both encryption and decryption

Optional public-key RSA and ECC engines

Done signal for interrupting the CPU

Test bench provided

Applications

- Embedded SSL/TLS applications

Synthesis Results

The size of the core depends on the core configuration (public key cryptography option is listed separately):

Cryptographic suites supported	Core size, K gates	System memory per connection, bytes
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	70	60
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA or TLS_RSA_WITH_AES_128_CBC_SHA	43	60
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	88	60

Public key cryptography size (requires dedicated memory):

- RSA – 15K gates, 6 x key length memory (for example, 1.5K bytes for RSA-2048).
- ECC – 16K gates for ECC-256, 26K gates for ECC-384, 5 x key length memory (160 bytes for ECC-256)

Export Permits

US Bureau of Industry and Security has assigned the export control classification number 5E002 to the encryption cores. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to the US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Verilog testbench (self-checking)
- Vectors for testbench
- Software development kit
- OpenSSL integration
- Expected results
- User Documentation

Contact Information

- IP Cores, Inc.
- 3731 Middlefield Rd.
- Palo Alto, CA 94303, USA
- Phone: +1 (650) 815-7996
- E-mail: info@ipcores.com
- www.ipcores.com