Trilinear

High-bandwidth Digital Content Protection

HDCP
ENCRYPTION-DECRYPTION ENGINE

The Trilinear Technologies High-bandwidth Digital Content Protection (HDCP) Encryption-Decryption Engine IP core implements the HDCP 1.3/2.3 digital stream cipher for both encryption and decryption operations. When used in combination with the Trilinear HDCP Authentication Software Stack running on a local processor, this IP core provides a complete, real-time solution for HDCP 1.x or HDCP 2.x protection of a digital link.

AT A GLANCE:

- Real-time encryption/ decryption
- 8k compression available for select applications
- Low gate count and low latency implementation
- Supports HDCP 1.3 and 1.4
  - R0, M0 hardware calculations
  - Optional hardware key interface for master key calculations
  - Host-free operation after initial authentication
- Supports HDCP 2.2/2.3
  - Hardware calculations for dkey0, dkey1, dkey2, and Ekh values
  - AES-128-compliant
- Fully integrated authentication management
- Source, sink, and repeater support
- Typical performance is 400 MHz in 12 nm
- Implementation resource usages:
  - Xlinx Kintex-7: 15K LUT, 6K FLOP
  - ASIC: 150K gates

Data in

Streaming interface using parallel data format for processing multiple symbols per clock cycle.

Data out

Low-latency streaming interface that parallels the input interface, providing consistent latency in both encrypted and plain text modes.

Host

32-bit AMBA Peripheral Bus (APB) 4 interface for configuration information and control.

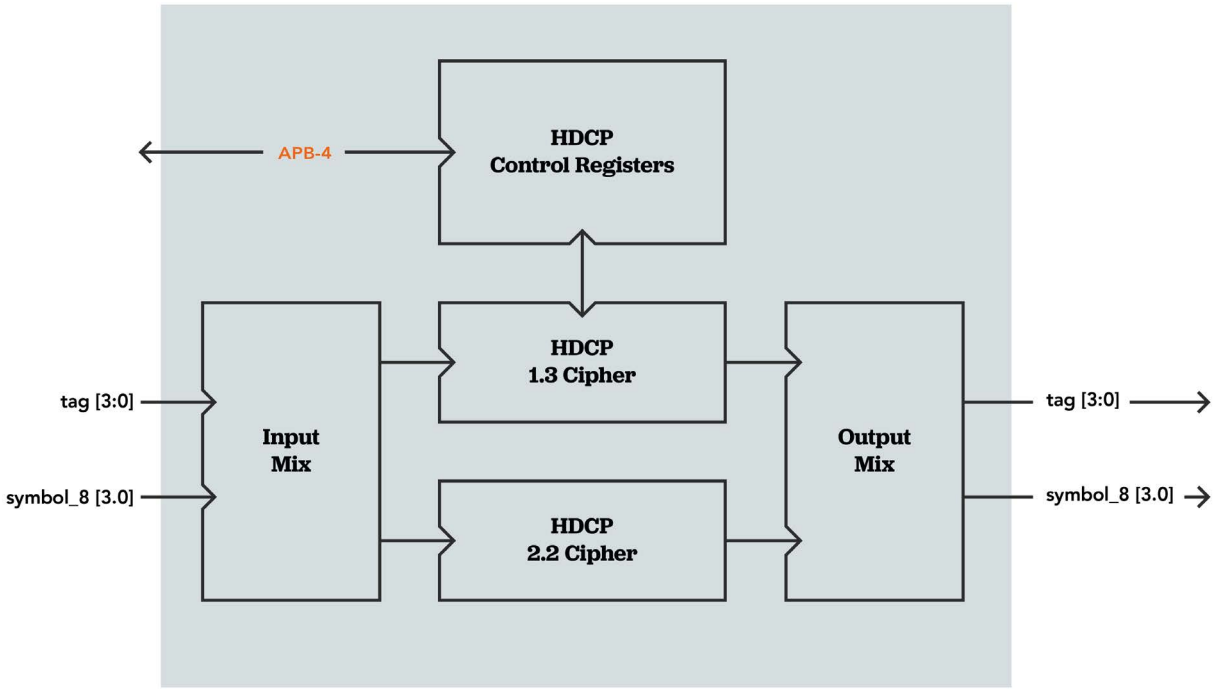

Figure 1. Block Diagram and Core Interfaces

Delivery & Availability

The HDCP Encryption-Decryption Engine IP core ships with a standards-compliant implementation of the HDCP Authentication protocol. The software provides hardware-accelerated and software implementations of all of the encryption algorithms to implement a complete system. The stack has been designed to meet the requirements of the HDCP Authentication speeds on a reasonable 32-bit microcontroller.

Verification Testing

Verification testing was completed using a bottom-to-top methodology. Testing is first performed at the module level and progresses up to system level. With the HDCP Encryption-Decryption Engine IP core, module-level testing consists of generating both randomized and corner case (boundary value) conditions.

Design Database

Trilinear Technologies delivers an extensive design database for the HDCP Encryption-Decryption Engine core. In addition to the synthesizable RTL IP core and extensive user-level verification environment, the database includes all the files required to implement the design on multiple platforms, including FPGA and ASIC technologies. Reference software drivers and applications are included, along with associated documentation to reduce the amount of time for software development. Files and data include:

- HDL source files for function design
- Fully functional models for block-level and top-level testing, including over 120+ tests in the user-level environment
- Functional specification
- Timing constraints summary document
- Generic SRAM simulation models
- C Reference Driver

READY?

Trilinear Technologies offers the HDCP Encryption-Decryption Engine IP core under several licensing models. Please contact Trilinear Technologies for pricing and additional information: **trilineartech.com**