General Description

HDCP Suite consists of hardware and software components implementing the HDCP 2.0 protocol.

The hardware components are fully synchronous and available as Verilog source. The software components are available in C language.

Key Features

Support for HDCP 2.0

Support for all HDCP configurations:

- HDCP Transmitter (-TX)
- HDCP Receiver (-RX)
- HDCP Repeater (-RPT)

Implementation of the HDCP Authentication protocol:

- Authentication and Key Exchange (AKE)
  - With Key Derivation
- Locality Check
- Session Key Exchange (SKE)
- Authentication with Repeaters

Data encryption:

- Utilizes HDCP Cipher (AES-128-CTR)
- Includes the Link Synchronization
  - Transmitter and Receiver utilize the counter information in the PES Private Data
- FIFO-like flow-through interface with flexible bit width; simple integration into the datapath.
- Microprocessor-friendly interface for programmable I/O is optional

Applications

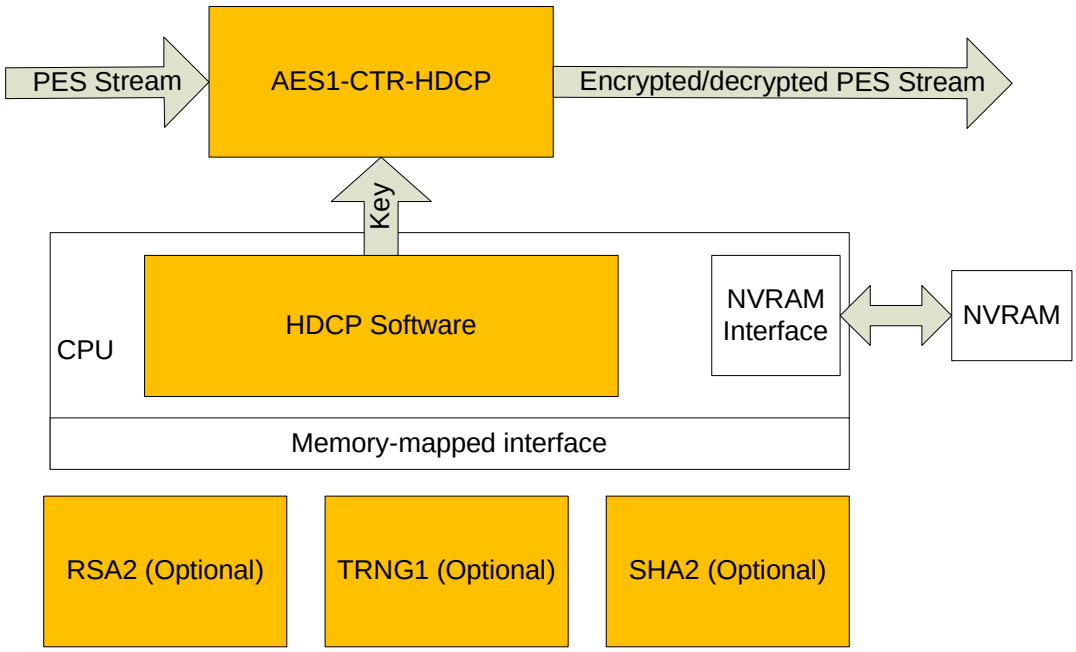
- Digital rights management (DRM)
- HDCP 2.0 implementations for generic wired and wireless interfaces

Components

- HDCP software written in C (CPU subsystem is not included)
- Hardware accelerators
  - AES1-CTR-HDCP: AES encryption/decryption capable of handling the PES streams
  - RSA2: An RSA hardware accelerator (optional, high-end CPUs can use the software implementation)
  - TRNG1: A true random number generator (optional, if entropy bits are available in the design, a software implementation can be used)
  - SHA2-256: A Sha-256 hash accelerator (optional, most CPUs can use the software implementation)

Function Description

The HDCPS suite includes hardware and software components. Supplied components are highlighted on the diagram below.



Implementation Details

Component	ASIC, NAND gates	Dedicated memory, bits	CPU code size, bytes	CPU data size, bytes	NVRAM, bytes
HDCP protocol			8KB	4KB	6KB
AES1-8CTR-HDCP	10K				
RSA2	12K	18K or 6K (note 1)			
SHA2-256	18K				
TRNG1	9K				
RSA software			5KB	3KB	
TRNG software			1.5KB		
SHA-256 software			2KB		

Notes:

1. RSA2 can either have 3072-bit support, or just 1024. In the latter case, the dedicated memory requirements are 3x times lower, yet RSA-3072 will be implemented in software (add the software modules size to the RAM/ROM requirements)

Export Permits

The core can be a subject of the US export control. It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing the AES encryption technology. See the IP Cores, Inc. licensing basics page, http://ipcores.com/exportinformation.htm, for links to US government sites and more details.

Deliverables

HDL Source Licenses

- Synthesizable Verilog RTL source code
- Source code for software
- Verilog testbenches for hardware components (self-checking)
- Vectors and expected results for testbenches
- Hardware models for software verification
- 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