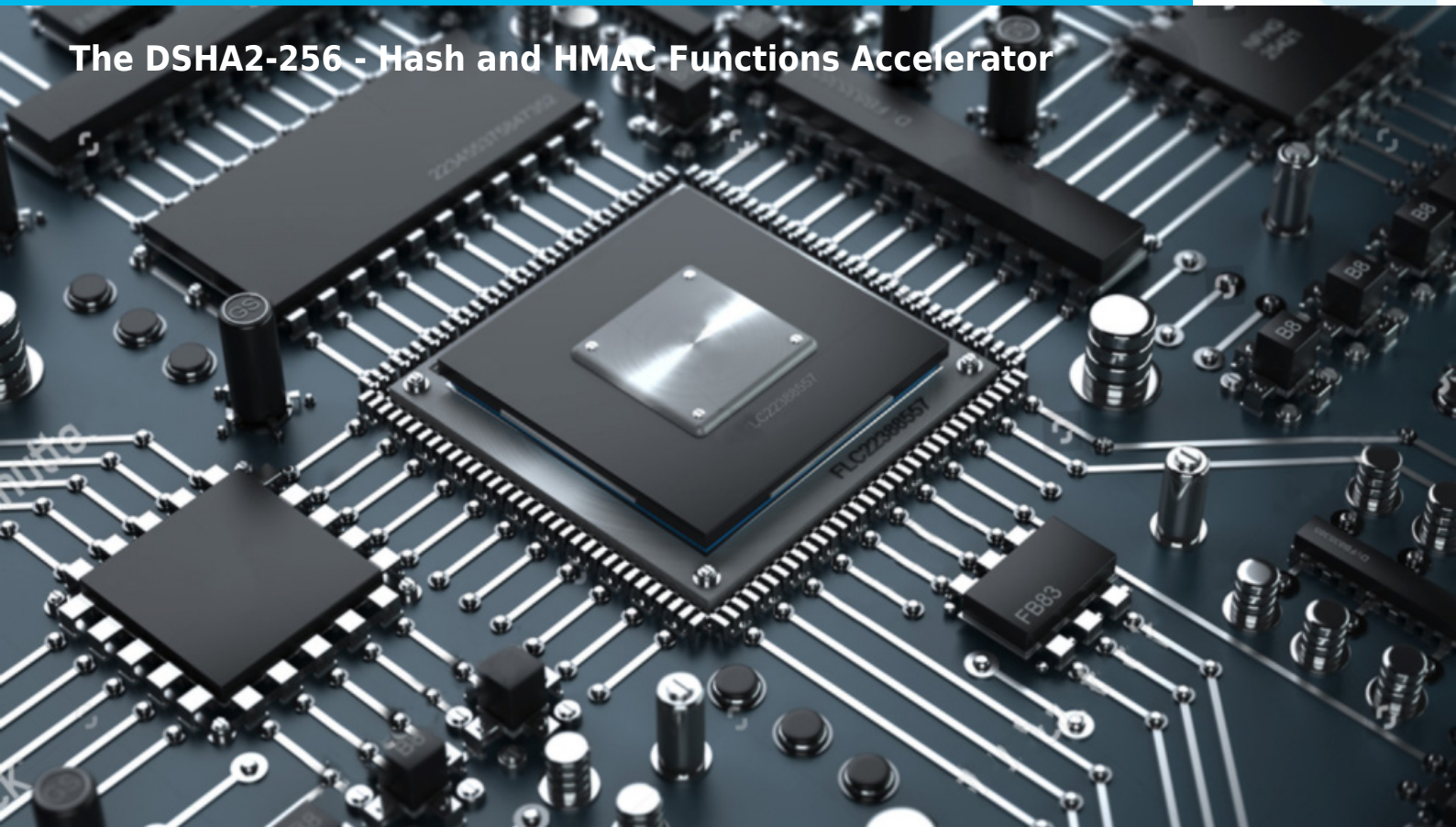




DSHA2-256



The DSHA2-256 - Hash and HMAC Functions Accelerator



COMPANY OVERVIEW

DCD-SEMI is a leading IP Core provider and a System-on-Chip design house. The company was founded in 1999 and since the very beginning has been focused on IP Core architecture improvements. Our innovative, silicon proven solutions have been employed by over 300 customers and with more than 500 hundred licenses sold to companies like Intel, Siemens, Phillips, General Electric, Sony and Toyota. Based on more than 70 different architectures, starting from serial interfaces to advanced microcontrollers and SoCs, we are designing solutions tailored to your needs.

IP CORE OVERVIEW

DSHA2-256 bridge to APB, AHB, AXI bus, it is a universal solution which **efficiently accelerates SHA2-256 hash function compliant with FIPS PUB 180-4**. It computes message digest in either **256 or 224 bit modes**. Allowed input message length is up to $2^{64} - 1$ bit. Depending on the core configuration it also natively **supports the SHA2-256 HMAC (Keyed-Hash Message Authentication Code), a cryptographic function defined in RFC 2104**. This IP is suitable for **authenticity and data integrity verification in digital signature protocols** and generally in **secure communication**. It might also be used in **accelerating of cryptocurrency computations**. What is more, it offers a **context swapping feature**, which might be used in complex systems with a task's preemption mechanism. Its other application can be software managed or custom HMAC scheme. SHA2 is a family of cryptography secure one-way compression functions based on Merkle-Damgard structure, the 256 version sequentially processes 512-bit input blocks during 64 rounds. From arbitrary length input message (maximum $2^{64} - 1$ bits) it produces fixed 256 or 224-bit length digest in a way, that it is practically infeasible to invert it (get an original message from its digest). Such property is called a one-way function. Cryptographic security of SHA2-256 is assumed at 128-bit level (112 bit in case of SHA2-224) which makes it appropriate for use in security applications. Some of these applications need to prove knowledge or possession of some secret data while computing message digest. For such authentication purpose, the HMAC function has been designed. It combines both secret key and cryptography secure hash function (like SHA2-256).

DCD's cryptographic system has been awarded as the Most Innovative IP Core of the Year during IP SoC China



DESIGN FEATURES:

All DCD's IP Cores are technology independent which means that they are 100% compatible with all FPGA & ASIC vendors e.g.

- **Altera / Intel,**
- **Xilinx / AMD,**
- **Lattice,**
- **Microsemi / Microchip,**
and others.

- **TSMC**
- **UMC**
- **SK Hynix**
and others.

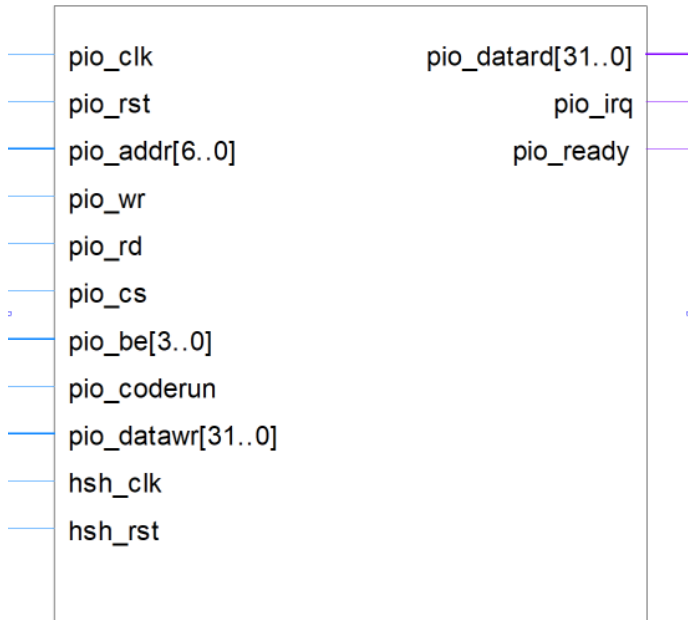
KEY FEATURES

- **Available IP configurations:**
 - **HASH:** Digest computing only
 - **CTX SWP:** Digest computing with context swapping support
 - **HMAC:** Digest and RFC 2104 compliant HMAC computing with context swapping support
- Moreover, each version can optionally support a binary length resolution of processed messages
- FIPS PUB 180-4 compliant SHA2-256 function
- RFC 2104 compliant HMAC mode native support
- SHA2 224 and 256 bit modes support
- Secure storage for precomputed HMAC keys
- Hash/HMAC context swapping
- Internal, automatic padding module
- Binary message resolution support
- Flexible data read/write modes
- AMBA AHB, AXI4, APB interface ready
- Software driver with OpenSSL/MbedTLS interface ready
- **Available system interface wrappers:**
 - **AMBA - APB / AHB / AXI Bus**
 - **Altera Avalon Bus**
 - **Xilinx OPB Bus**

APPLICATIONS

- Digital signature
- Data integrity
- Key derivation
- TLS/SSH/PGP IPsec communication

HARDWARE DESCRIPTION



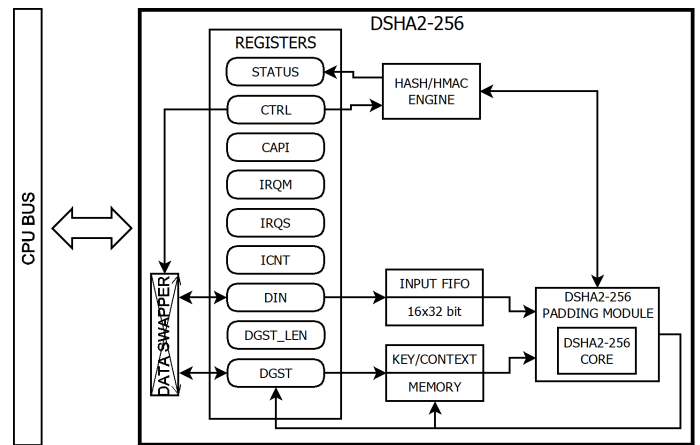
DESIGN FEATURES:

All DCD's IP Cores are technology independent which means that they are 100% compatible with all FPGA & ASIC vendors e.g.

- **Altera / Intel,**
- **Xilinx / AMD,**
- **Lattice,**
- **Microsemi / Microchip,**
and others.

- **TSMC**
- **UMC**
- **SK Hynix**
and others.

BLOCK DIAGRAM



PERFORMANCE

The following table gives a survey about the Core area and performance in **AMD XILINX®** devices after Place & Route of exemplary devices:

HMAC version

Device			FMax PIO	FMax HSH
Kintex UltraScale+	2314LUT	930FF	100MHz	230MHz
Zynq 7000	2274LUT	932FF	100MHz	160MHz
Artix 7	2279LUT	932FF	100MHz	90MHz

HASH version

Device			FMax PIO	FMax HSH
Kintex UltraScale+	1727LUT	913FF	100MHz	230MHz
Zynq 7000	1845LUT	913FF	100MHz	185MHz
Artix 7	1837LUT	913FF	100MHz	90MHz

CTX_SWP version

Device			FMax PIO	FMax HSH
Kintex UltraScale+	2104LUT	920FF	100MHz	230MHz
Zynq 7000	2142LUT	919FF	100MHz	160MHz
Artix 7	2142LUT	919FF	100MHz	90MHz

DELIVERABLES

The list of deliverables consists of:

- Source code:
 - VERILOG Source Code
 - Software driver in C with OpenSSL/MbedTLS interface ready
- VERILOG test bench environment
 - Active-HDL automatic simulation macros
 - ModelSim automatic simulation macros
 - Tests with reference responses
- Technical documentation

- HDL core specification
- Software driver documentation
- Synthesis scripts
- Example application
- Technical support
 - IP Core implementation support
 - 12 months of maintenance
 - Delivery of the IP Core and documentation updates
 - Phone & email support
 - Design consulting

LICENSING

Comprehensible and clearly defined licensing methods without royalty-per-chip fees make use of our IP Cores easy and simple.

- **Single-Site license option** - dedicated to small and middle sized companies which run their business at one place.
- **Multi-Site license option** - dedicated to corporate customers which operate at several locations. The licensed

product can be used at selected company branches. In all cases the number of IP Core instantiations within a project and the number of manufactured chips are unlimited. There are no restrictions regarding the time of use.

There are two formats of the delivered IP Core that you can choose from:

- Verilog or VHDL RTL synthesizable source code (called HDL Source code)
- FPGA EDIF/NGO/NGD/QXP/VQM (called Netlist)

HDL Source code is suitable for ASIC and FPGA projects. The Netlist license is intended for FPGA projects only.

CONTACT

DCD-SEMI Headquarters:

Wroclawska 94, 41-902 Bytom, POLAND

E-mail: info@dcd-semi.com

tel.: +48 32 282 82 66

fax: +48 32 282 74 37

Distributors:

Please check: dcd-semi.com/contact-us/