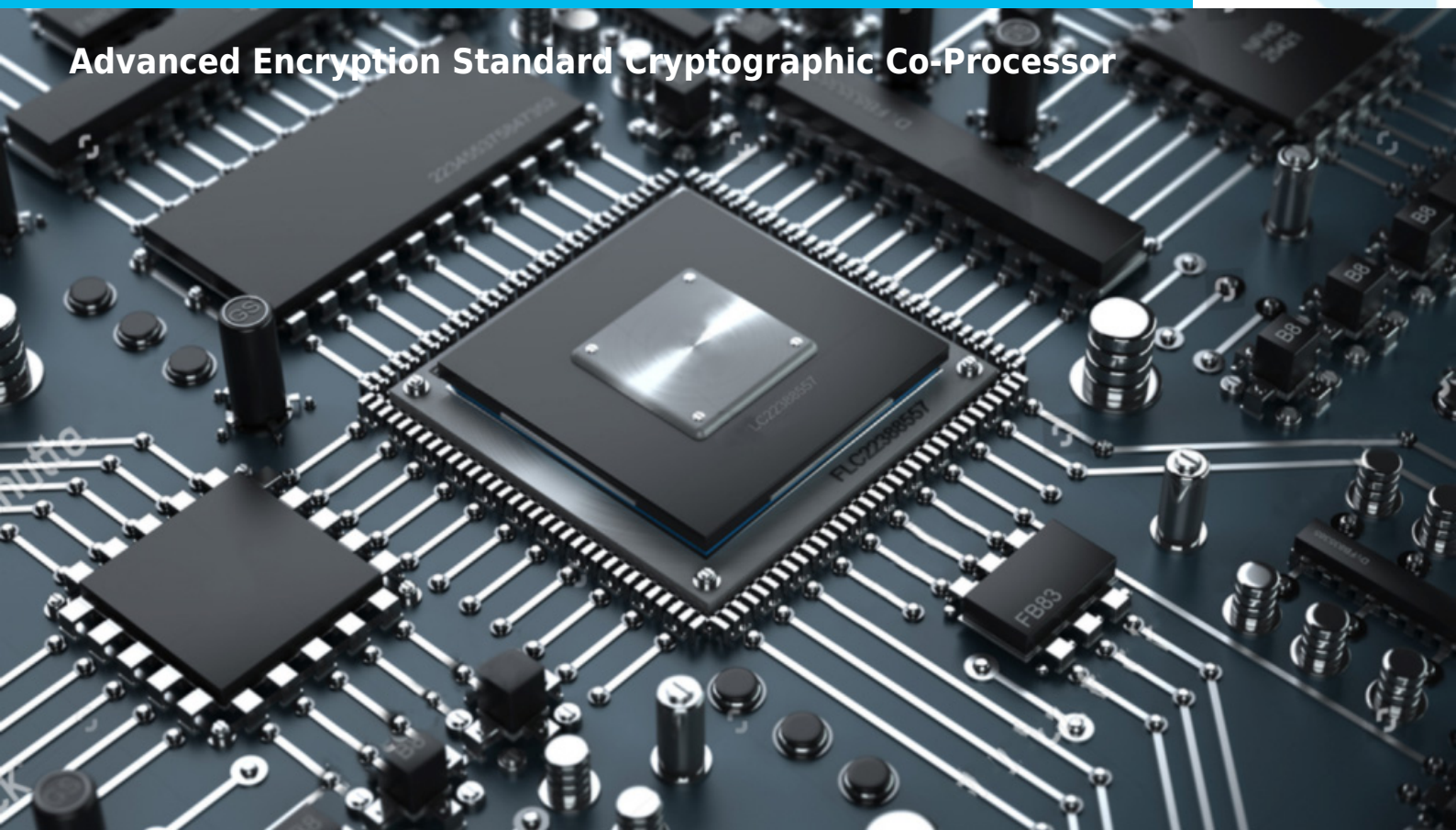
DIGITAL CORE DESIGN

DAES

Advanced Encryption Standard Cryptographic Co-Processor



COMPANY OVERVIEW

Digital Core Design 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, Philips, 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

DAES bridge to APB, AHB, AXI bus, it is a cryptographic co-processor which implements Rijndael encryption algorithm compliant with FIPS 197 Advanced Encryption Standard. AES is a widely deployed block cipher in security solutions from IoT devices to cloud servers. Its implementation in hardware brings significant benefits on fields of security and performance over software one.

KEY FEATURES

- Support for 128 and 256 key bit length
- Support for ECB, CBC, CFB, OFB, CTR block cipher modes
- Internal key expansion module
- Flexible data read/write modes
- **Available system interface wrappers:**
  - **AMBA – APB / AHB / AXI Bus**
  - **Altera Avalon Bus**
  - **Xilinx OPB Bus**

BLOCK CIPHER MODES

DAES supports the following block cipher modes:

- Electronic Codebook (ECB),
- Cipher Block Chaining (CBC),
- Cipher Feedback (CFB),
- Output Feedback (OFB),
- Counter (CTR).

Most modes require a unique binary sequence, often called an initialization vector (IV), for each encryption operation.

PERFORMANCE

The following table gives a survey about the Core area and performance in **XILINX®** devices:

Device	Registers	LUTs	F_{max}
Artix-7	1 658	3 100	90

DELIVERABLES

The list of deliverables consists of:

- Source code:
  - VERILOG Source Code
  - Bare-metal C software driver
- VERILOG test bench environment
  - Active-HDL automatic simulation macros
  - ModelSim automatic simulation macros
  - Tests with reference responses
- Technical documentation
  - HDL core specification
- Synthesis scripts
- Example application
- Technical support
  - IP Core implementation support
  - 3 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:
– VHDL or Verilog 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

Digital Core Design Headquarters:
Wroclawska 94, 41-902 Bytom, POLAND
E-mail: info@dcd.pl
tel.: 0048 32 282 82 66
fax: 0048 32 282 74 37
Distributors:
Please check: dcd.pl/contact-us/