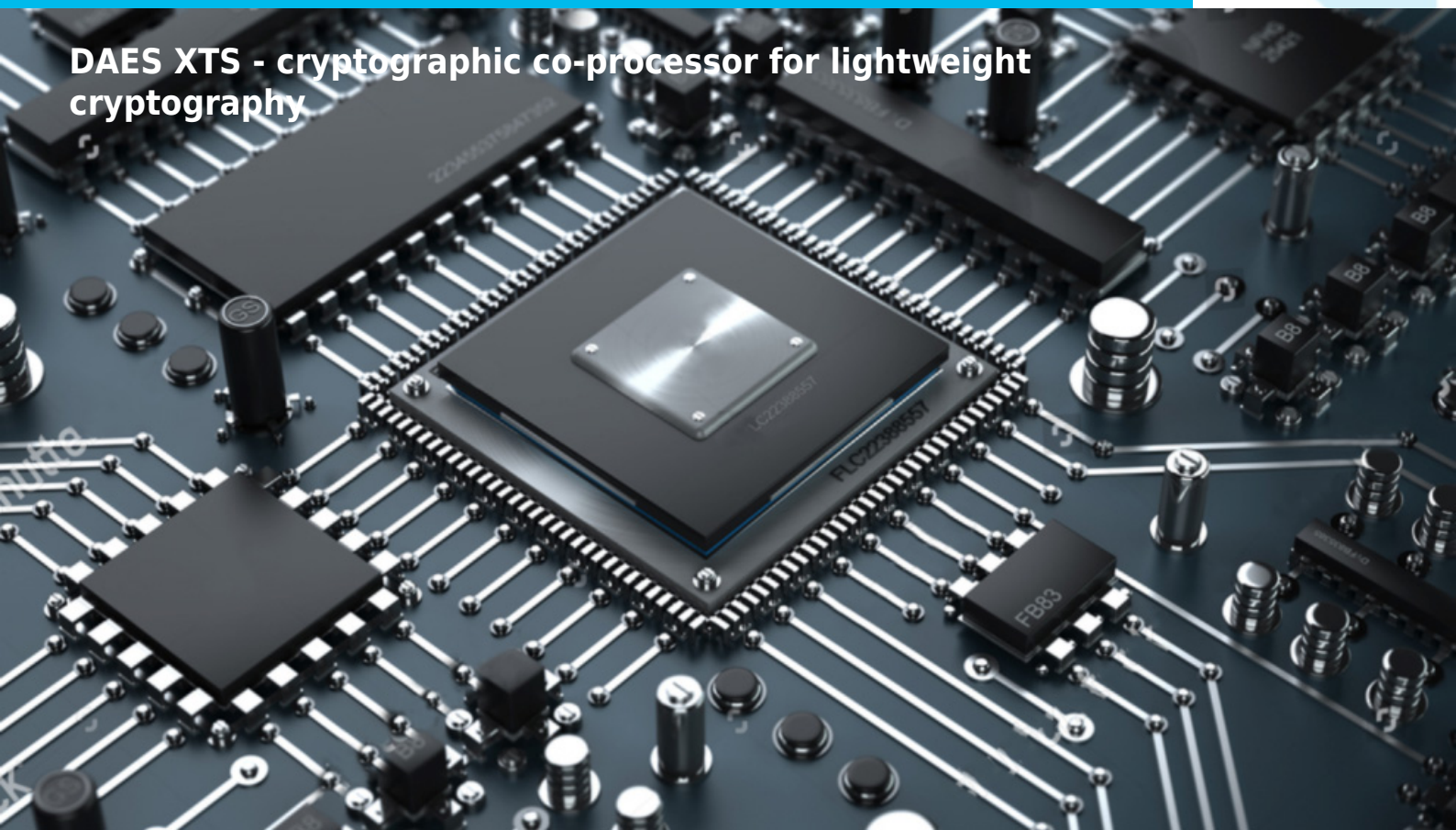
DIGITAL CORE DESIGN

DAES XTS



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 XTS IP Core from Digital Core Design is a compact cryptographic co-processor designed to seamlessly implement the Rijndael encryption algorithm in compliance with **FIPS 197 Advanced Encryption Standard**, specifically in XTS mode (by **IEEE Std 1619-2007 standards**).

Tailored for IoT and embedded devices applications requiring robust hardware disk encryption, this solution excels with its support for encrypted memories such as FLASH or RAM, thanks to the random data access block function.

The DAES XTS is an ideal choice for security-conscious environments, ranging from IoT devices to cloud servers, owing to the widespread adoption of the AES block cipher. Its hardware-based implementation offers substantial advantages in both security and performance compared to software-based alternatives. It is important to note that Ciphertext-Stealing mode is currently not supported; therefore, the DAES XTS expects memory sectors to be aligned to multiples of 128-bit blocks.

Furthermore, **seamless integration** is possible with a diverse array of **SPI memory** controllers, enhancing the **versatility and compatibility of the DAES XTS for a wide range of applications**. Elevate your security measures with this lightweight yet powerful cryptographic solution.

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

- Support AES-XTSmode—IEEE Std 1619-2007 standard compliance
- Support 128 and 256-bit key size
- Random memory block access support
- Internal key expansion module
- Minimal resource usage for embedded systems
- Optional embedded memory interface ready wrapper

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 of **INTEL FPGA®** devices:

Device	ALMS	REGs	ALUT	MEM	FMAX
Cyclone V	2660	1723	3486	1920bit	125MHz
Max 10		1601	4663 LEs	1920bit	120MHz

DELIVERABLES

- Source Code
- Verilog Source Code
- Verilog test bench environment
- Questa, Model Sim, Active-HDL, automatic simulation macros
- Tests with reference responses Technical documentation
- Installation note
- HDL core specification

- Datasheet
- Technical support

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.: +48 32 282 82 66
fax: +48 32 282 74 37
Distributors:
Please check: dcd.pl/contact-us/