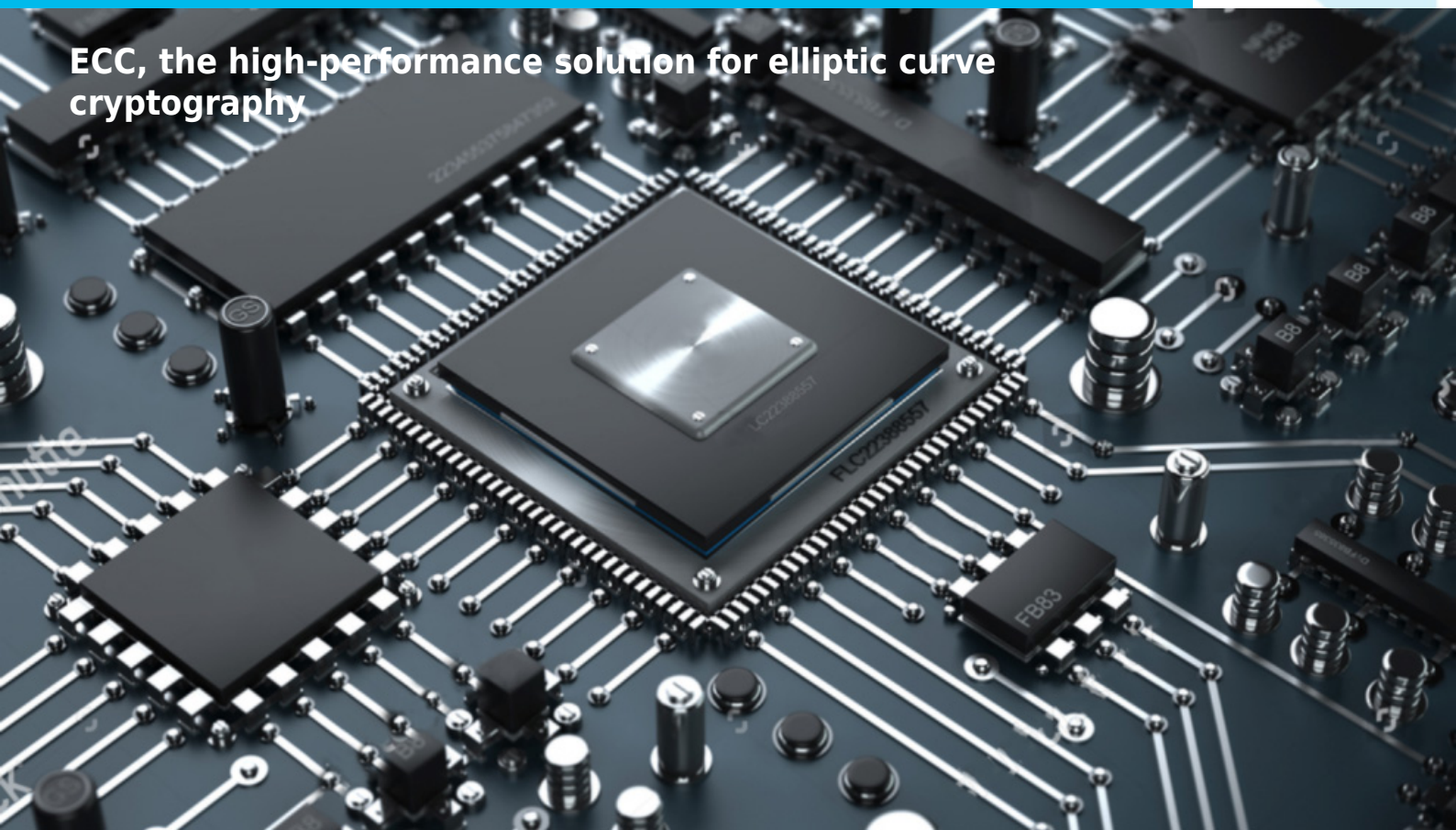
DIGITAL CORE DESIGN

# ECC



## 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

**Safety & security** meet the best **size/performance ratio**... ECC verification IP Core!

Our ECC IP Core represents a cutting-edge solution that brings the power of elliptic curve cryptography to your systems. Designed with versatility and performance in mind, this IP Core supports a range of essential algorithms, including point multiplication, ECDSA signature generation, and ECDSA signature verification.

With the ability to perform point multiplication, our ECC IP Core enables efficient and secure elliptic curve operations. Point multiplication is a fundamental operation in elliptic curve cryptography, allowing for scalar multiplication of a point on the curve. This operation forms the basis for various cryptographic protocols, including key generation, key agreement, and digital signatures.

In addition to point multiplication, our ECC IP Core facilitates ECDSA signature generation. ECDSA (Elliptic Curve Digital Signature Algorithm) is a widely adopted digital signature scheme that provides robust authentication and data integrity. By leveraging the computational strength of elliptic curves, our IP Core enables rapid and reliable generation of ECDSA signatures, empowering secure digital transactions and communications.

Furthermore, our ECC IP Core includes support for ECDSA signature verification. This capability allows for the efficient verification of ECDSA signatures, ensuring the integrity and authenticity of digital data. By employing optimized elliptic curve computations, our IP Core enables fast and accurate verification, essential for establishing trust and preventing fraudulent activities.

With our ECC IP Core integrated into your systems, you gain a versatile and high-performance solution for elliptic curve cryptography. Its comprehensive support for point multiplication, ECDSA signature generation, and ECDSA signature verification empowers you to implement robust cryptographic protocols, secure digital transactions, and protect sensitive data with ease. Experience the power and efficiency of elliptic curve cryptography through our advanced ECC IP Core.

- Supported algorithms:
  - Point multiplication
  - ECDSA signature generation
  - ECDSA signature verification

**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

- Supported Elliptic Curves
  - NIST SECP P-256 R1
  - NIST SECP P-384 R1
  - Koblitz SECP P-256 K1
  - Koblitz SECP P-384 K1
  - Brainpool P-256 R1
  - Brainpool P-384 R1
  - Brainpool P-512 R1
  - other/custom curves optional support
- Optional Side Channel Attacks countermeasures
- Input/Output EC point verification
- Fully synthesizable, synchronous design
- Highly configurable in terms of performance and resource consumption
- Minimum operation delay at 200 MHz:
  - Point multiplication:
    - EC256: 2.5 ms
    - EC384: 5.0 ms
  - ECDSA signature generation
    - EC256: 2.6 ms
    - EC384: 5.2 ms
  - ECDSA signature verification
    - EC256: 3.1 ms
    - EC384: 6.3 ms
- Estimated resource usage
  - from 30k to 110k NAND gates

## APPLICATIONS

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

## HARDWARE DESCRIPTION

## PERFORMANCE

***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.***

## 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:
– 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/