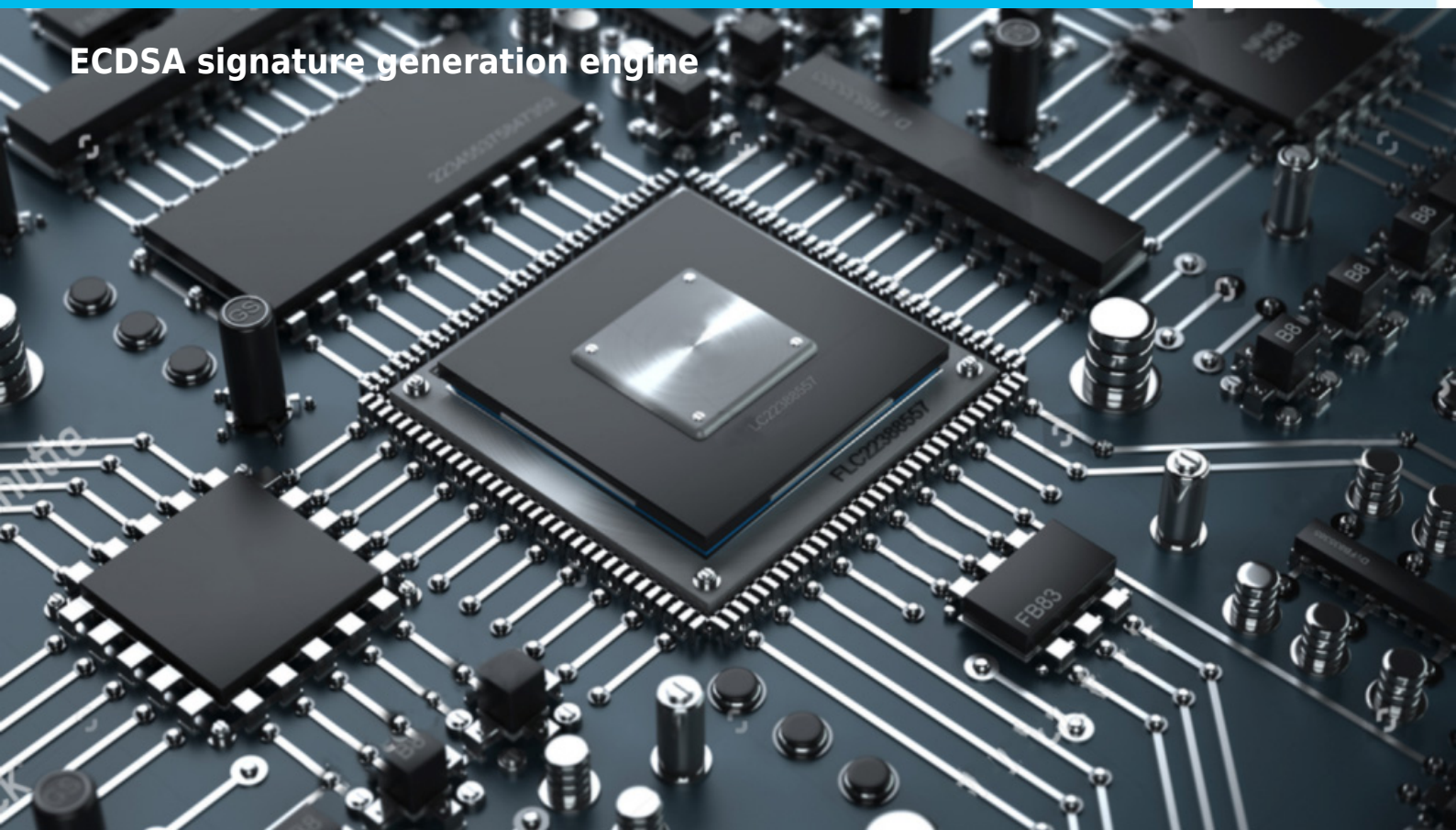
DIGITAL CORE DESIGN

ECDSA SIGN

ECDSA signature generation engine



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

When **safety & security** meet the best **size/performance ratio**... ECDSA IP Core

Elliptic curves form the foundation of cutting-edge public-key cryptography, serving as a crucial component for secure digital signatures and robust key agreement protocols, such as the esteemed Diffie-Hellman scheme. Leveraging the mathematical properties of elliptic curves, CryptOne emerges as a formidable IP Core specifically engineered to execute elliptic curve cryptography operations with unparalleled efficiency and reliability.

Adhering to the rigorous guidelines set forth by the Federal Information Processing Standards (FIPS) 186 standard, our CryptOne solution not only meets but exceeds the stringent security requirements demanded by modern electronics. By supporting a diverse array of elliptic curves, CryptOne empowers users with the flexibility to select curves that align with their specific cryptographic needs, ensuring compatibility with a wide range of cryptographic systems.

What sets CryptOne apart is its ingenious design and remarkable scalability achieved through the utilization of DCD's exceptional IP core architecture. This groundbreaking architecture enables the implementation of CryptOne with an incredibly compact silicon footprint, maximizing resource utilization while minimizing overhead costs. Furthermore, CryptOne's superior processing speeds deliver lightning-fast cryptographic operations, enabling rapid and seamless integration within high-performance computing environments.

With CryptOne's innovative IP core at the heart of your cryptographic infrastructure, you can harness the power of elliptic curves with unmatched efficiency, reliability, and compliance, ushering in a new era of secure communications and data protection.

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

To provide you with the most accurate and detailed insights about the Microsemi performance, we encourage you to get in touch with us directly.

Please feel free to contact us at **info@dcd.pl**. Our dedicated team will be more than happy to assist you with any inquiries you may have.

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/