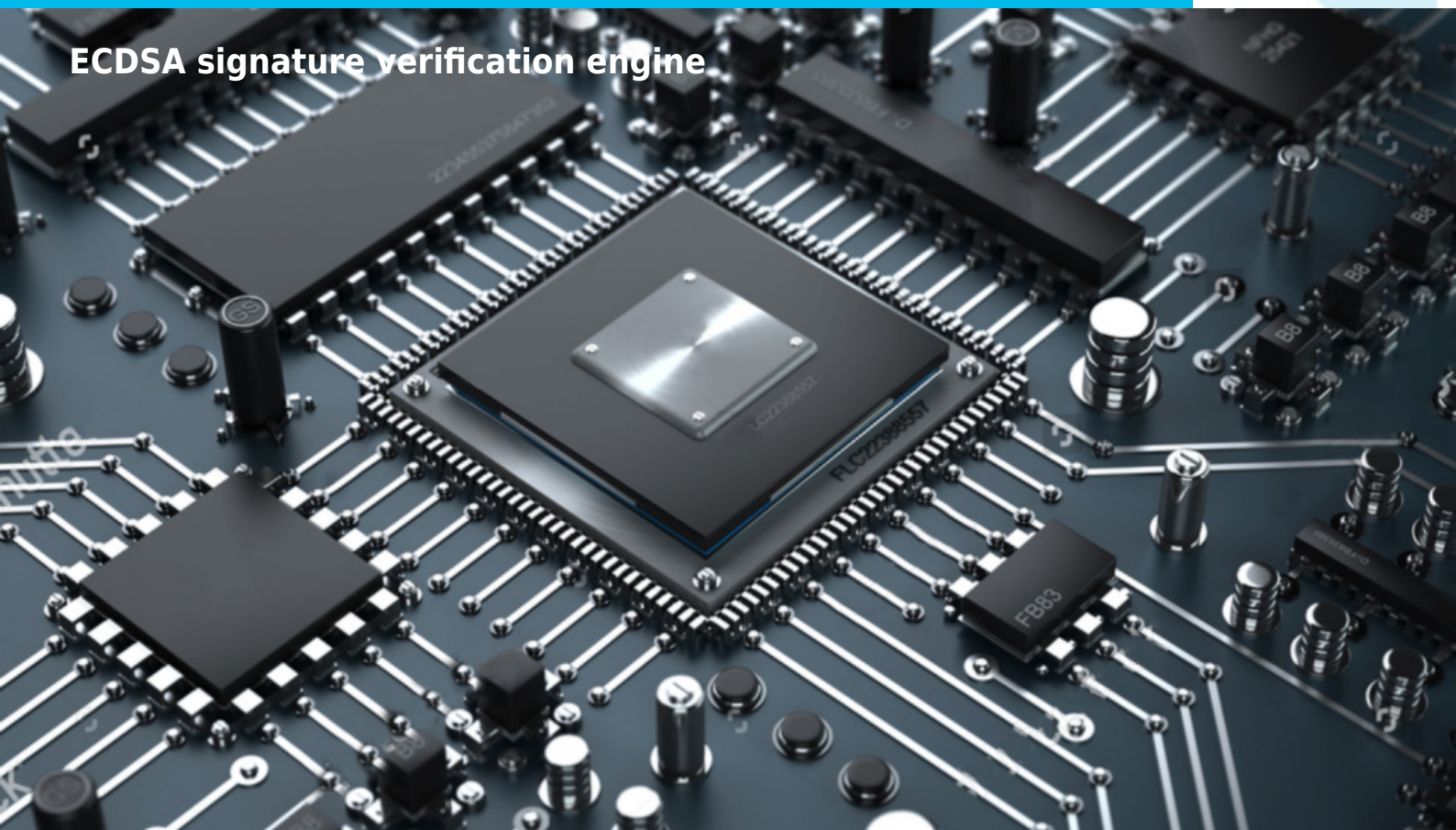
DIGITAL CORE DESIGN

ECDSA VERIFY 384



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

In addition to its support for various elliptic curves, CryptOne's prowess extends to the widely acclaimed Elliptic Curve Digital Signature Algorithm (ECDSA). ECDSA, based on the principles of elliptic curve cryptography, is a cornerstone of modern cryptographic systems and provides a secure and efficient method for digital signature generation and verification.

CryptOne's implementation of ECDSA leverages the inherent mathematical properties of elliptic curves to ensure the integrity, authenticity, and non-repudiation of digital data. The algorithm operates by generating a digital signature using the private key associated with an elliptic curve key pair. This signature can then be verified by employing the corresponding public key, thus establishing the authenticity and integrity of the signed data.

Underpinning CryptOne's ECDSA operations is a suite of robust and optimized algorithms and protocols. These algorithms efficiently perform the necessary mathematical computations involving elliptic curves, resulting in swift and accurate digital signature generation and verification processes. By adhering to the FIPS 186 standard, CryptOne's ECDSA implementation meets stringent security requirements, ensuring compatibility and interoperability with a wide range of cryptographic systems.

Furthermore, CryptOne's IP core architecture plays a crucial role in optimizing ECDSA performance. Its scalable design allows for the efficient execution of ECDSA operations, enabling high-speed processing while maintaining a minimal silicon footprint. This unique combination of scalability and performance empowers CryptOne to deliver exceptional cryptographic performance, making it an ideal solution for resource-constrained environments where computational efficiency is paramount.

With CryptOne's advanced ECDSA capabilities, organizations can confidently secure their digital communications, transactions, and sensitive data by leveraging the robustness and efficiency of elliptic curve cryptography. By integrating CryptOne into their cryptographic infrastructure, users can harness the power of ECDSA to ensure the utmost security and trustworthiness of their digital interactions.

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

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.***

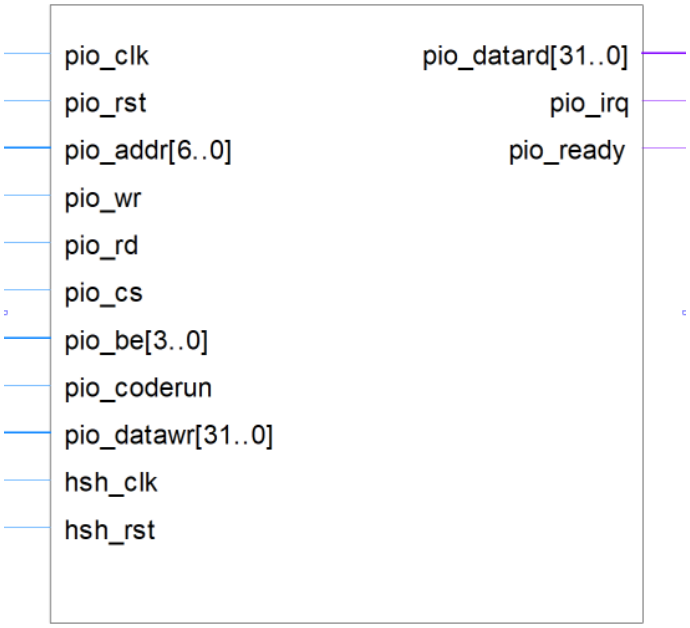
KEY FEATURES

- 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



- 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

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.

PERFORMANCE

To provide you with the most accurate and detailed insights about the ASIC 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

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/