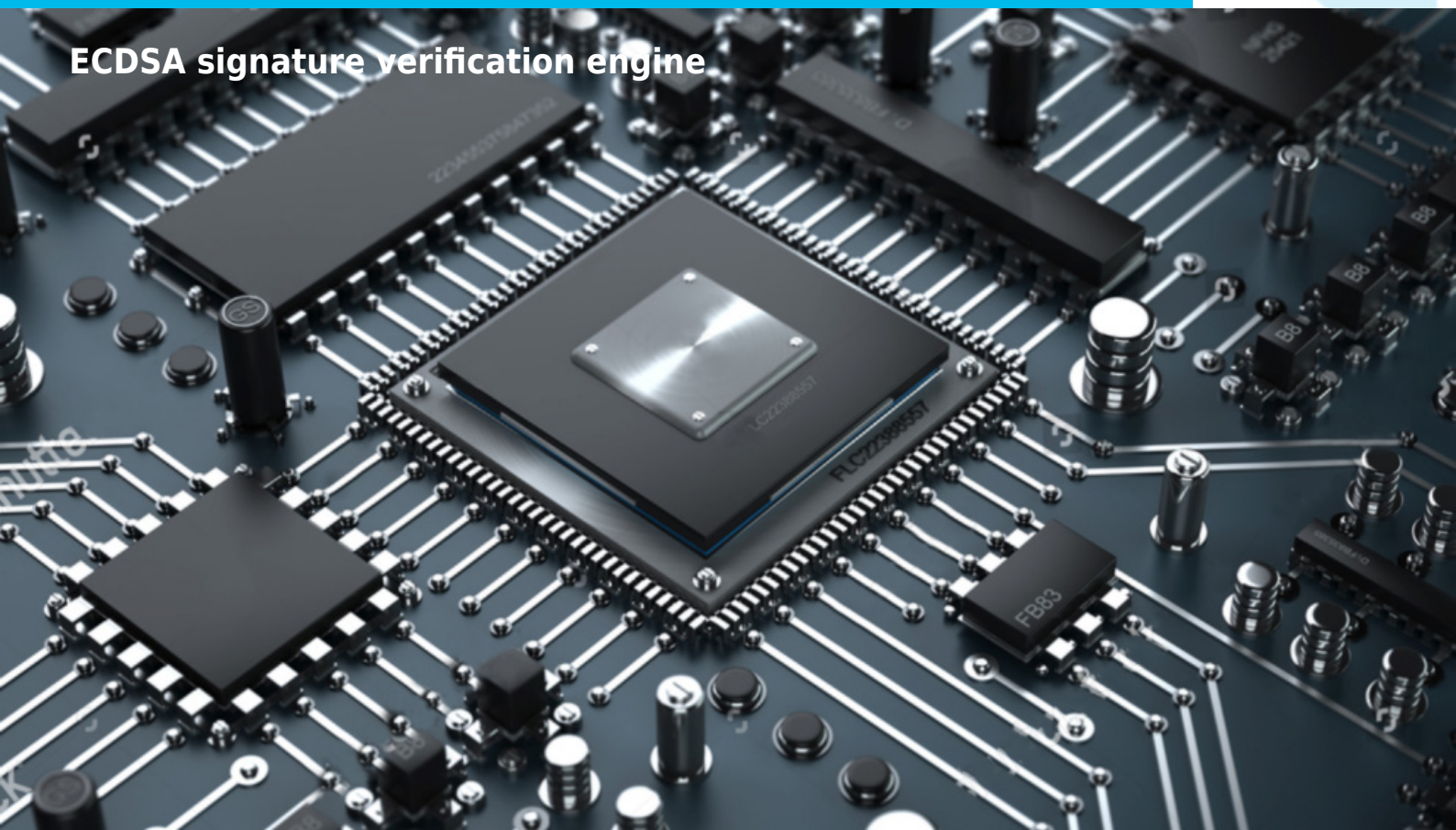
DIGITAL CORE DESIGN

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

CryptOne ECDSA IP Core — High-Performance Elliptic Curve Digital Signatures

Beyond supporting a broad range of elliptic curves, **CryptOne** excels in implementing the **Elliptic Curve Digital Signature Algorithm (ECDSA)**—a cornerstone of modern cryptographic systems. ECDSA provides a secure, efficient, and standards-compliant method for **digital signature generation and verification**, ensuring data authenticity, integrity, and non-repudiation.

CryptOne's ECDSA engine leverages the mathematical properties of elliptic curves to execute cryptographic operations with **maximum efficiency and precision**. Digital signatures are generated using private keys and verified with corresponding public keys, providing a robust mechanism for **trusted communications, secure transactions, and protected data storage**.

Optimized Algorithms and High-Speed Architecture

At its core, CryptOne integrates **highly optimized algorithms** for elliptic-curve arithmetic, delivering **swift and accurate signature generation and verification**. Full compliance with **FIPS 186** guarantees stringent security standards, ensuring interoperability across diverse cryptographic systems.

The IP core's **scalable architecture** maximizes throughput while maintaining a **minimal silicon footprint**, making it ideal for **resource-constrained SoCs, FPGAs, and embedded platforms**. High-speed ECDSA processing combined with compact design allows engineers to achieve **optimal size/performance ratios**, reducing CPU load and enabling secure, low-latency operations.

Secure, Efficient, and Future-Proof

By integrating CryptOne's ECDSA IP Core into their designs, organizations can confidently **protect digital communications, authenticate sensitive transactions, and safeguard critical data**. Its combination of **robust elliptic-curve security, high efficiency, and FIPS compliance** makes it a go-to solution for **IoT, automotive, industrial, and high-assurance embedded systems**.

Harness the power of **CryptOne ECDSA** to implement **fast, reliable, and standards-compliant elliptic-curve digital signatures**, ensuring the highest levels of security and trustworthiness for modern electronics.

ALL DCD'S IP CORES ARE TECHNOLOGY AGNOSTIC, ENSURING 100% COMPATIBILITY WITH ALL FPGA AND ASIC VENDORS.

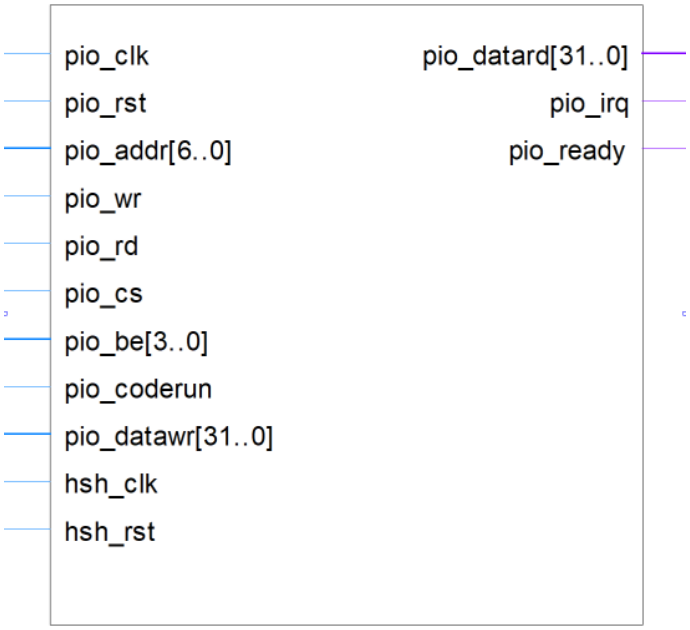
For further details, email info@dcd.pl.

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

HARDWARE DESCRIPTION

Copyright © 1999 - 2026 DCD - DCD-SEMI Sp. z o.o. All Rights Reserved.
All trademarks mentioned in this document are the property of their respective owners.



APPLICATIONS

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

PERFORMANCE

For precise LATTICE performance insights, reach out to us at info@dcd.pl. Our dedicated team is ready to assist you with any inquiries.

DELIVERABLES

- HDL Source Code
- Testbench environment
  - Automatic Simulation macros
  - Tests with reference responses
- Synthesis scripts
- Technical documentation
- 12 months of 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.

– Remote Access license option – allows authorized users to access and use the licensed product from a remote location.

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.

The IP is delivered in HDL Source code suitable for ASIC and FPGA projects.

CONTACT

DCD-SEMI Sp. z o.o. 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/

Copyright © 1999 - 2026 DCD - DCD-SEMI Sp. z o.o. All Rights Reserved.
All trademarks mentioned in this document are the property of their respective owners.