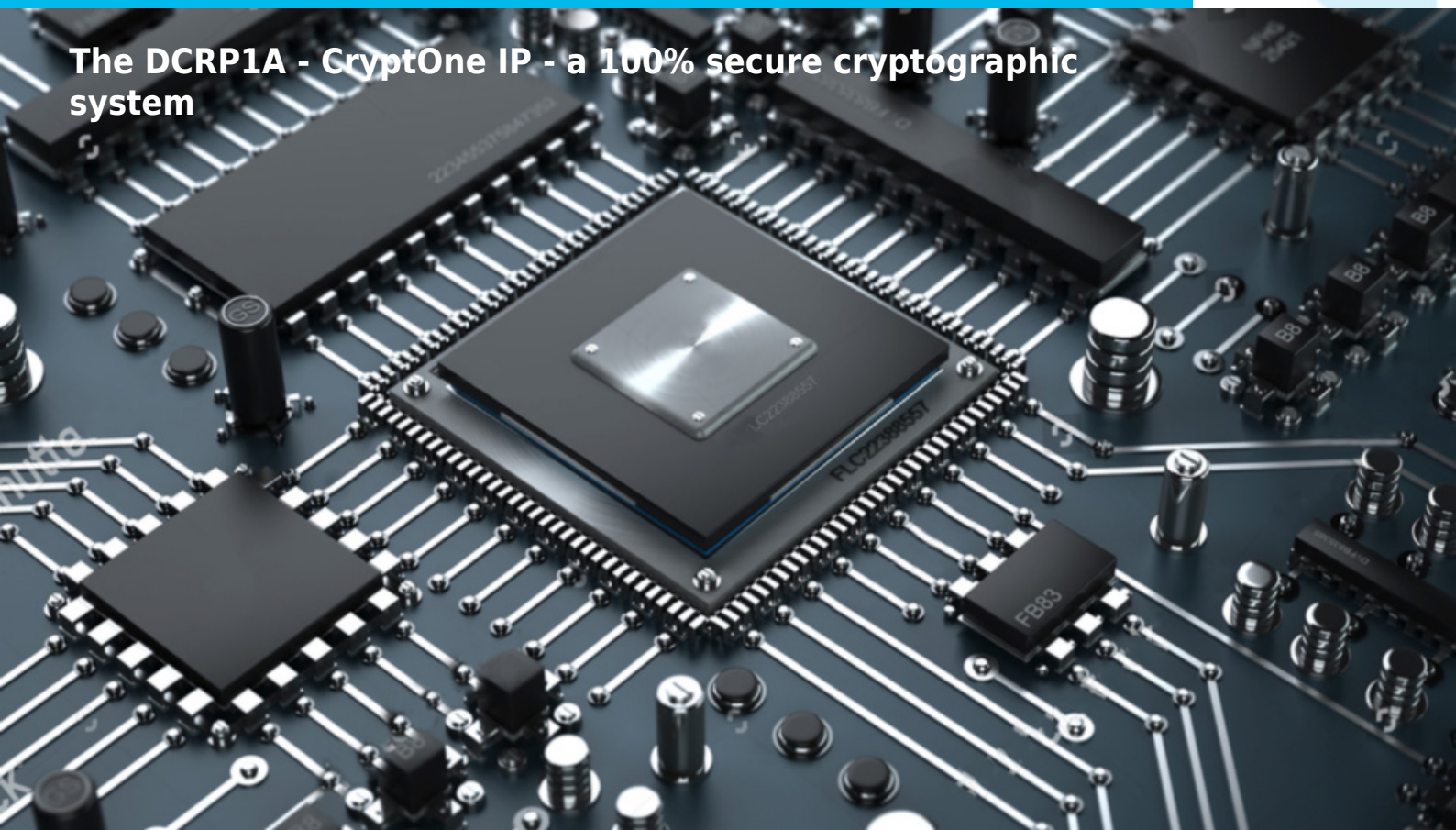
DIGITAL CORE DESIGN

DCRP1A

The DCRP1A - CryptOne IP - a 100% secure cryptographic system



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 – a **100% secure cryptographic system** based on more than 20 years of DCD's market experience. It is a universal and fully scalable solution that is able to boost asymmetric cryptographic algorithms like:

- **Digital Signature**,
- **modular exponentiation (RSA)**
- **RSA** (keys up 4096 bits) with **CRT option**
- **Diffie-Hellman**
- **Elliptic Curve Cryptography (ECC) in GF(p)**
- **Miller-Rabin test**

DCD's cryptographic solutions offer various configurations, tailored to the project needs. During the tests, the DCRP1's utilized up to 25% fewer logic cells, with the same performance – when compared to competitive designs. And when it's optimized for speed, it's achieved up to 50% higher performance, than competitive designs.

What does that mean? Ultimate performance:

Elliptic Curve NIST-P256 operations performance **at 200 MHz**
EC point mul: 2.5 ms
ECDSA sign: 2.6 ms
ECDSA verify: 3.2 ms

The energy-efficient architecture of CryptOne IP core enables the usage of a **very small silicon footprint** with **high processing speeds**. It can be provided with various different interfaces, including **AMBA AHB**, **AXI4,** and **APB**. The very intuitive interface allows fast and straightforward system integration. The core is resistant to timing attacks and contains optional DPA countermeasures. CryptOne system is universal and fully scalable, accelerating up to **4096 bits** big number arithmetic operations such as: modular multiplication, subtraction, addition, and shifts. Cryptographic instructions support provides the ability to boost public key algorithms like **RSA, Diffie-Hellman, and ECC**.

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

- CryptOne programmed algorithms:
  - Constant time **modular exponentiation**
  - Constant time, **parallel modular exponentiation CRT**
  - Constant time **ECDSA sign/verify**
  - Constant time **ECDH**
  - Constant time **elliptic curve point multiplication**
  - No branch **modular multiplicative inverse**
  - No branch **GCD**
  - Constant time **modular reduction**
  - Constant time **multiplication**
  - Constant time **division**
- Cryptographic algorithm applications:
  - *ECDSA, ECDH*
  - *RSA key generation*
  - *RSA Sign/Verify/Encrypt/Decrypt*
  - *Diffie-Hellman schemes*
  - *Miller-Rabin Primality check*
- System applications:
  - *Client-server communication*
  - *Sensor networks*
  - *SSL/TLS stacks*
  - *IoT devices*
  - *Embedded security/ID devices*
- AMBA AHB, AXI4, APB interface ready
- Rapid & easy development with delivered API
- Patent pending architecture
- Algorithms resistant against SPA and timing attacks
- CryptOne elliptic curves with native support:
  - NIST P-192
  - NIST P-224
  - NIST P-256
  - NIST P-384
  - Koblitz P-192
  - Koblitz P-256
  - Koblitz P-384
  - Brainpool P-256
  - Brainpool P-384
  - Brainpool P-512
  - Other/custom curves optional support
- Software support:
  - **OpenSSL** engine
  - **MbedTLS** port
  - **OS independent** crypto library

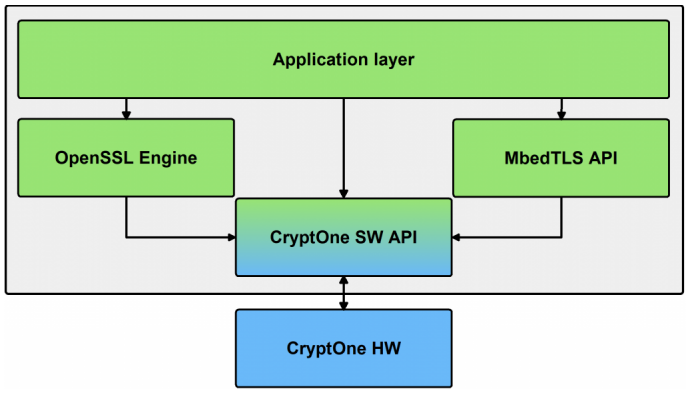
OFFERED PRODUCTS

- CryptOne RSA:
  - Constant time **modular exponentiation**
  - Constant time, **parallel modular exponentiation CRT**
  - Secure RSA key generation with:
    - No branch **modular multiplicative inverse**
    - No branch **GCD**
    - Constant time **multiplication**
    - Constant time **division**
  - **OpenSSL** engine, **MbedTLS** port
  - **OS independent** crypto library
- CryptOne EC:
  - Constant time **ECDSA sign/verify**
  - Constant time **ECDH**
  - Constant time **elliptic curve point multiplication**
  - Native support for most popular elliptic curves
  - **OpenSSL** engine, **MbedTLS** port
  - **OS independent** crypto library
- CryptOne TLS
  - Both EC and RSA versions support

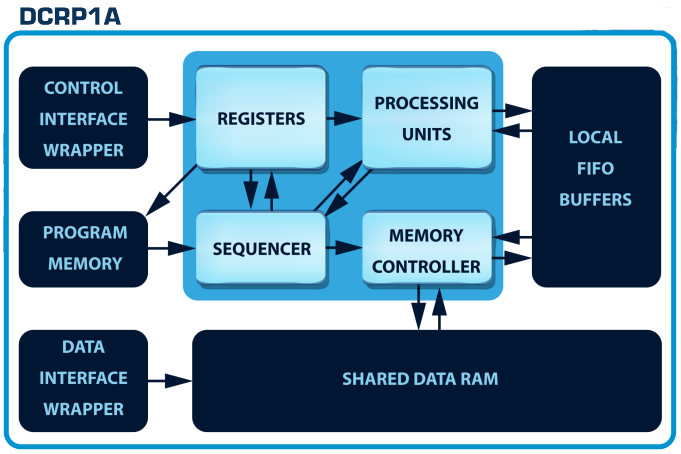
CONFIGURATION

Several parameters of the CryptOne can be easily adjusted to requirements of a dedicated application and technology. The configuration of the System can be effortlessly done, by changing appropriate constants in the package. There is no need to change any parts of the HDL source code.

SOFTWARE STACK



BLOCK DIAGRAM



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:

- C software drivers with API
- Silicon proven architecture
- Hardware code:
  - VERILOG Source Code or
  - FPGA Netlist
- VERILOG test bench environment
- Technical documentation
- Synthesis scripts
- 12 months of free technical support included

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/