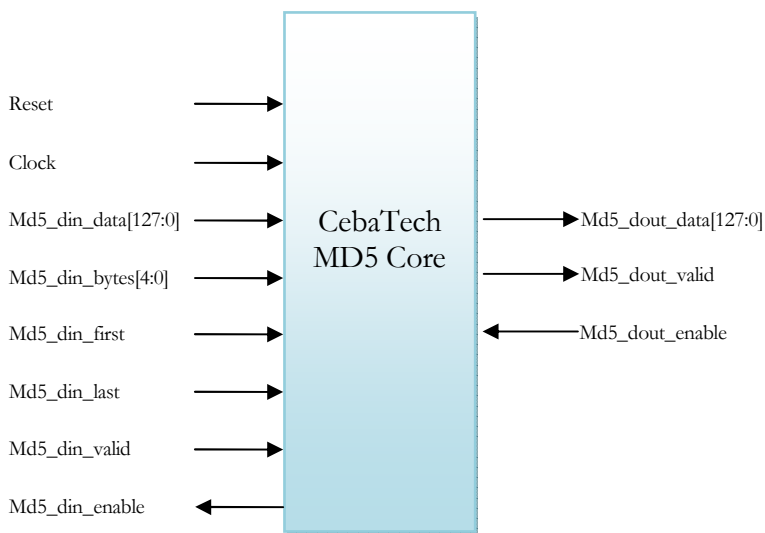


Overview

CebaTech's MD5 cores are a direct hardware embodiment of Ron Rivest's original software implementation as defined in RFC 1321, enabling a state of the art FPGA or ASIC solution for cryptographic hash function with 128-bit hash value. CebaTech's hardware implementation of MD5 is in the form of standalone soft cores that perform the cryptographic hash function. CebaTech's MD5 cores precisely follow the data formats defined by the software algorithm.

CebaTech's MD5 cores are designed to reduce the processing overhead of high-speed data hashing.



Deliverables

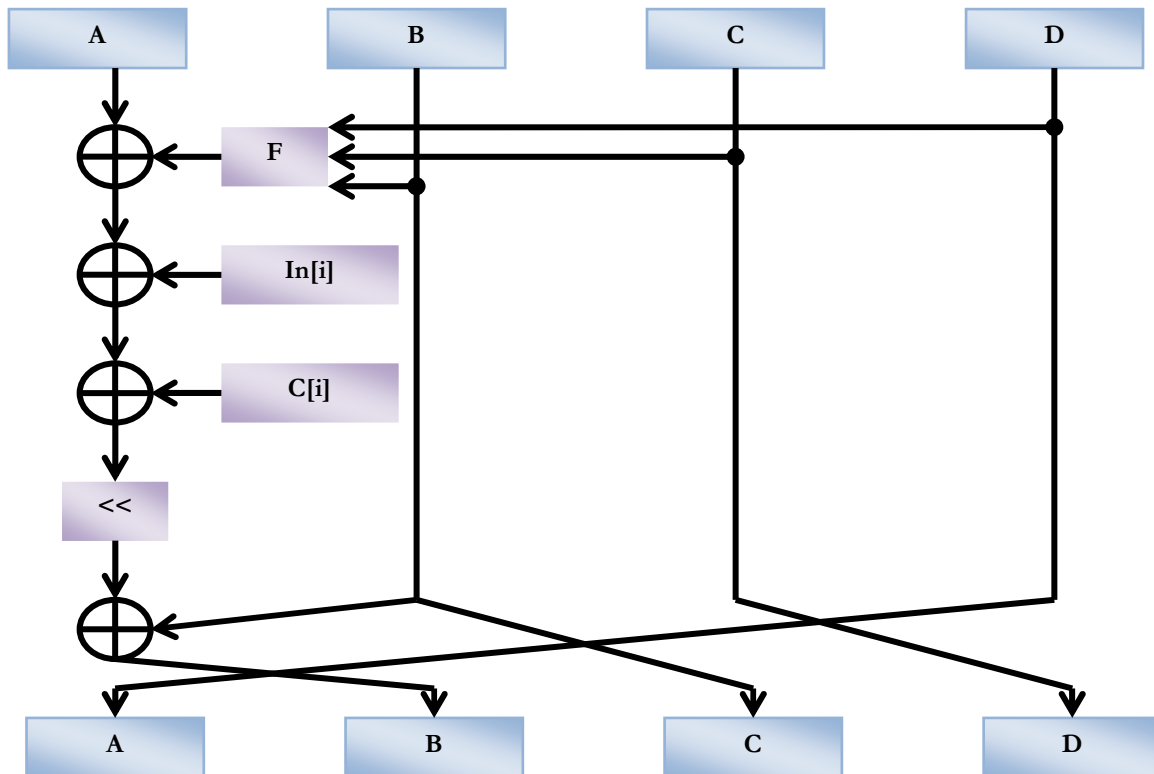
- Synthesizable Verilog™ RTL Source.
- Comprehensive User's Guide.
- Simulation Environment and Scripts.
- Test Files.

CebaTech's MD5 Features

- Self-contained, standalone soft core that performs the hash function.
- Fully compliant with RFC1321.
- Fully conformant with Ron Rivest's software algorithm.
- Suitable for FPGA and ASIC targets.
- Fully synchronous design.
- Auto padding.

MD5 Hash Cryptography

MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. The MD5 algorithm operates on a 128-bit state which is divided into 32-bit words. The states are initialized to certain fixed constant. After initialization, the algorithm operates on a 512-bit block of data. The message is padded so that its length is divisible by 512 bits. There are total of 16 rounds of operation, each round is based on 4 computations as defined in RFC 1321. The following diagram summarizes the MD5 transformation:



At the end of the computation, the module generates a 128-bit message digest that can be used, for example, to authenticate the content of the message.

MD5 Core applications:

MD5 has been used for data integrity, authentication, and digital signatures in many networks and storage systems. MD5 can also be found in electronic funds transfers and storage applications both for authentication and data integrity.

Resource Requirements

CebaTech's MD5 IP core targets both ASIC or FPGA applications. CebaTech's unique ESL flow allows timing, area and performance optimizations based on customer's requirements. For information related to your specific application needs, please contact us at sales@cebatech.com.

About CebaTech
Headquartered in Eatontown, NJ, CebaTech, Inc. is a privately held, venture-backed company focused on developing ESL tools and intellectual property modules that accelerate the development and realization of complex software algorithms in silicon. Information about the company and its products may be found at www.cebatech.com

This document contains information proprietary to CebaTech Inc. CebaTech retains all intellectual property rights in all products identified in this document. The products described in this document are subject to continuous development and all information is supplied strictly "as is" with no warranties implied or expressed and CebaTech, Inc shall not be liable for any loss or damage arising from the use of any information contained in this document. CebaTech, The Software to Silicon Company, are trademarks or registered trademarks of CebaTech Inc. in the United States and other countries. All other trademarks and registered trademarks are the property of their respective owners.