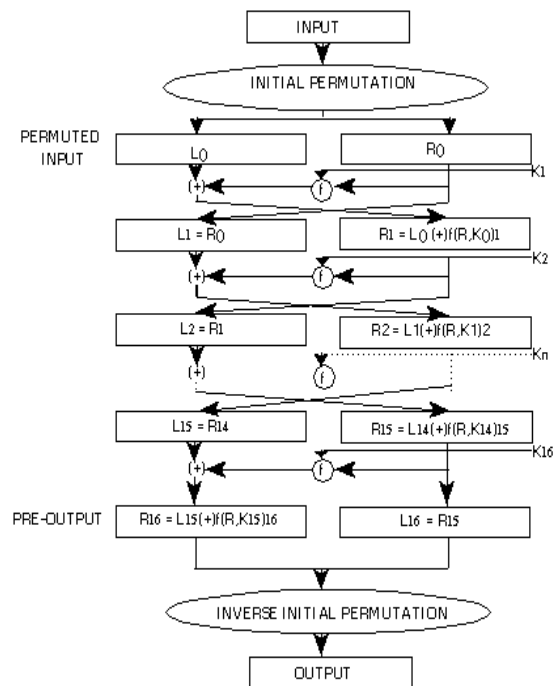


DES

Engine Data Sheet Module

Summary

The DES Engine is a low power, low cost hardware co-processor, which implements the Data Encryption Standard (DES) algorithm. The Engine is compatible with the C*CORE Bus and performs both encryption and decryption. As a trade-off between size (cost) and performance, the DES engine performs 64 bit encryption or decryption. The DES module can easily be used to perform the Triple DES (3DES) algorithm, which provides even greater protection



DES Block Diagram

Features

- Low power synthesizable design
- 32-bit C*CORE interface
- 64 bit DES encryption/decryption
- Support Triple-DES algorithm with 128 (112) bits or 192(168) bits key
- Support ECB mode and CBC mode
- Two 32 bit input data registers and two 32 output data registers
- Two 32 bit encryption key registers
- One 32bit initial vector register
- Data process speed up to 27.83MBps@80Mhz for DES
- Data process speed up to 11.64Mbps@80Mhz for Triple-DES

Performance and Characteristics

- Frequency (WCS): 100 MHz
- Die Size: 0.058 mm²
- Process: 0.18μm (WCS, 1.62V, 120°)

Application Examples

- Smart Card
- Security Chips
- Network Security
- Secure Communications

Availability

- Q1, 2008

To obtain more information about the DES or other C*Core™ products, please contact the C*Core Technology Co., Ltd. by phone: 0512-68091377, email: support@china-core.com or web: <http://www.china-core.com>.

C*Core™ is a trade mark of C*Core Co., Ltd.