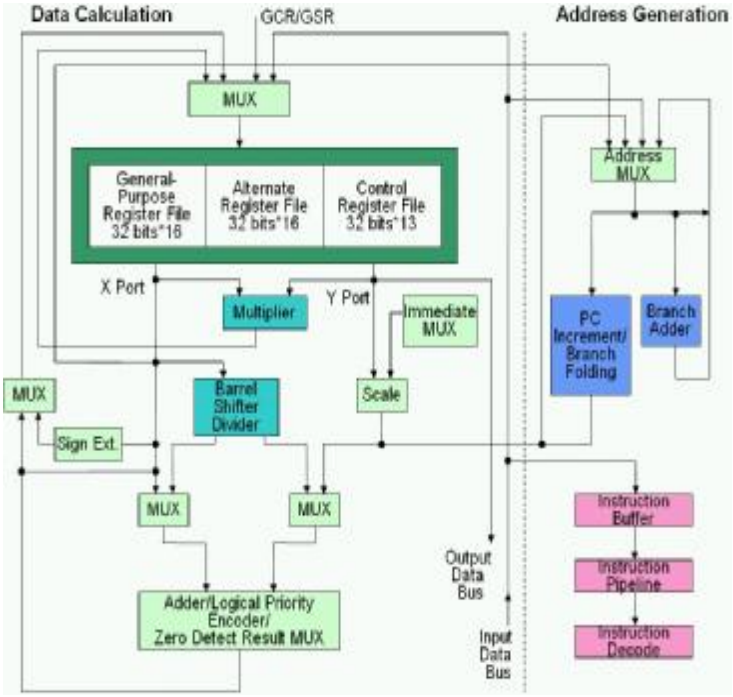
Secure RISC Core CS322D

Data Sheet

Summary

The CS322D is a 32-bit RISC core designed specifically for secure applications[#]. The CS322D is a member of the C*Core™ 32-bit RISC core family. In addition to providing most of the C310 core features, the CS322D incorporates advanced techniques to enable secure functionality, including a memory protection unit (MPU) integrated with the core. The MPU module provides additional security features to the CS322D core, which include flexible and powerful access protection modes, data encryption/decryption and address scrambling. It enhances protection against unauthorized access to sensitive data by providing two fixed and eight super-user programmable memory regions.



[#] Note: Because the CS322D core has a OnCE™ JTAG/Debug interface, which can be used to re-program or bypass the MPU, the CS322D is not considered a very secure core. The purpose of the CS322D is to enable building a test-chip for developing the secure application software, which is then embedded in another chip, which employs the CS322 core, which is secure (no debug interface).

Core Features

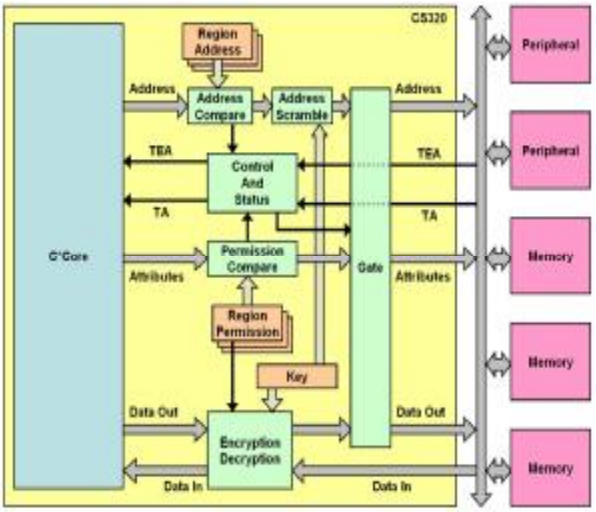
- Low power secure RISC core
- 32-bit load/store architecture
- Highly optimized pipeline
- Single-cycle 32x16 multiplier
- Fixed-length 16-bit instructions
  - Mostly single-cycle execution
  - Two-cycle branch execution
- 16 32-bit general purpose registers
- 13 32-bit control registers
- C*Bus MLB bus architecture
  - Support byte/halfword/word access
  - Optional AMBA wrapper
- Debug support via JTAG-based OnCE™ Design
- Fast interrupt support
  - 16 32-bit alternate registers for fast context switching
  - Vectored/auto-vectored interrupts
  - 128 interrupt/exception vectors
- Powerful security features
  - Memory Protection Unit
  - Data encryption
  - Address scrambling
  - Programmable access protection
- Debug support via JTAG-based OnCE™ Design
- Extendable simulator for application software development and secure debugging

The CS322D replaces the CS320D core, with which it is 100% backward compatible. The CS322D has a new 'secure-window' MPU protection mode, which is needed for secure Guomiban (国密办) software execution. The CS322D has better performance than the CS320D and can be implemented in FPGA.

C*Core Technology Co., Ltd.
http://www.china-core.com
Tel/Fax：0512－68091372/68096251
Email：support@china-core.com

CS322D MPU Features

- Memory Encryption Unit (MEU) provided to protect sensitive data from attack
- MPU features can only be enabled/disabled by super-user
  - Programmable regions disabled after reset by default, must be explicitly enabled by the super-user
  - Exception Vector Table/OS and MPU Control Space regions always protected
- Eight super-user programmable regions
  - Variable region size: 1Kbyte to 4Gbyte
  - Can be based anywhere in the 4Gbyte memory map
  - Region base address automatically aligned to the region size
  - Programmable data and address encryption/decryption
  - Flexible access permissions:
    - Super-user/user access
    - Read/write access
    - Execute (instruction fetch) access
- Regions allowed to overlap (strictest access permissions enforced for overlapped regions)
- One super-user access region for Exception Vector Table and Operating System (OS)
  - Fixed size: 4Kbyte
  - Fixed location: 0x00000000
  - Data and address encryption
  - Fixed access permission
    - Super-user read/write/ execute access only
- One super-user access region for the MPU Control Space
  - Fixed size: 64Kbyte
  - Fixed location: 0xFFFF0000
  - Fixed access permission
    - Super-user read/write access only
- Programmable 32-bit data and address encryption key
- Status register contains attribute and region details of access violations



CS322D Performance and Characteristics (example)

Process:	Hejian 0.18µm
Frequency (WCS)**:**	80MHz
Die Size:	0.75 mm^2
Power (TYP)**:**	TBD

The CS322D core is typically delivered as a square-shaped hard-macro, using 5 metal layers (50% of metal 5 is available for on-chip route). The figures above are speed-optimized implementation examples. The CS322D is available in a range of technologies, and various speed and area/power optimized versions, while other implementations are available on request.

Application Examples

- Smart Cards
- Banking
- Security Keys
- SIM Cards

Availability

- Q1, 2008

*To obtain more information about the CS322D or other C*CORE™ products, please contact the C*Core Technology Co., Ltd. by phone: 0512-68091372, email: support@china-core.com or web: http://www.china-core.com.*

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