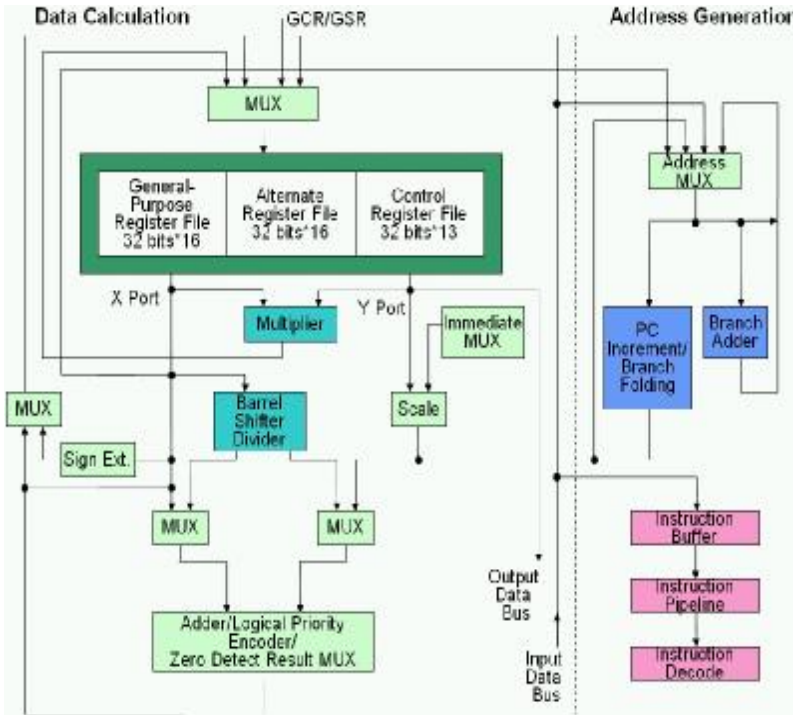


# Secure RISC Core CS320 Data Sheet

## Summary

The CS320 is a 32-bit RISC core designed specifically for secure applications. The CS320 is a member of the C\*Core™ 32-bit RISC core family. In addition to providing most of the C310 core features, the CS320 incorporates advanced techniques to enable secure functionality. It also includes a



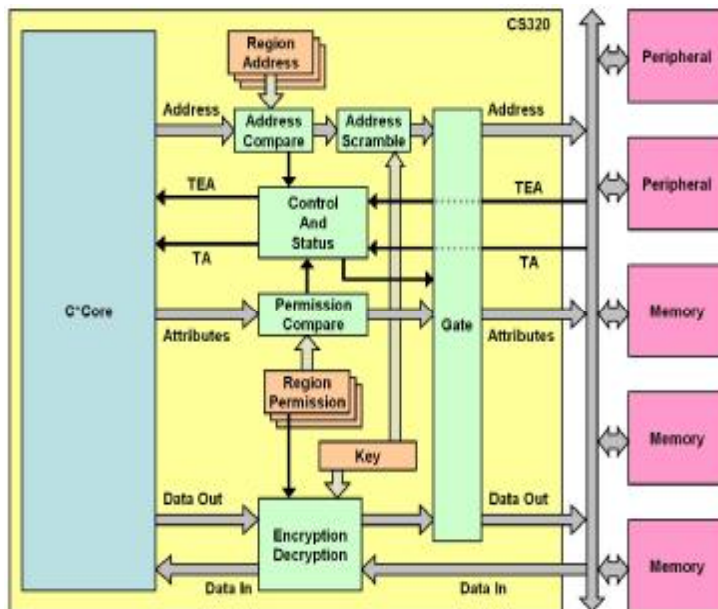
memory protection unit (MPU) integrated with the core. The MPU module provides additional security features to the CS320 core, which include flexible and powerful access protection modes, data encryption/ decryption and address scrambling, etc. It further enhances protection against unauthorized access to sensitive data by providing two fixed and eight super-user programmable memory regions. The CS320 hard-macro incorporates advanced techniques to protect the core from various forms of attack.

## Core Features

- Ø Low power secure RISC core
- Ø 32-bit load/store architecture
- Ø Highly optimized pipeline
- Ø Single-cycle 32x16 multiplier
- Ø Fixed-length 16-bit instructions
  - † Mostly single-cycle execution
  - † Two-cycle branch execution
- Ø 16 32-bit general purpose registers
- Ø 13 32-bit control registers
- Ø C\*Bus MLB bus architecture
  - † Support byte/halfword/word access
  - † Optional AMBA wrapper
- Ø Fast interrupt support
  - † 16 32-bit alternate registers for fast context switching
  - † Vectored/auto-vectored interrupts
  - † 128 interrupt/exception vectors
- Ø Powerful security features
  - † Memory Protection Unit
  - † Scrambled and optimized layout for enhanced security
  - † Irreversible and secure test mode
- Ø Extendable simulator for application software development and secure debugging

## CS320 MPU Features

- Ø Memory Encryption Unit (MEU) provided to protect sensitive data from attack
- Ø 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
- Ø 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
- Ø Regions allowed to overlap (strictest access permissions enforced for overlapped regions)
- Ø 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
- Ø 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
- Ø Programmable 32-bit data/ address encryption key
- Ø Status register contains attribute and region details of access violations



## CS320 Performance and Characteristics

**Process:**

Ø HHNEC 0.25µm/2.25V/125°C

Ø HHNEC 0.18µm/1.62V/125°C

**Frequency (WCS):**

Ø 40MHz (50MHz Max)

Ø 66MHz (80MHz Max)

**Power Consumption:**

Ø 0.34mW/MHz (3.6µW Leak)

Ø 0.14mW/MHz (18.1µW Leak)

**Die Size:**

Ø 0.99mm<sup>2</sup>

0.55mm

**Application Examples**

Ø Smart Cards

Ø Banking

Ø Security Keys

Ø SIM Cards

**Availability**

Ø Q2, 2003

*To obtain more information about the CS320 or other C\*CORE™ products, please contact the C\*Core Technology Co., Ltd. by phone: 0512-68091377, email: [support@china-core.com](mailto:support@china-core.com) or web: <http://www.china-core.com>.*

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