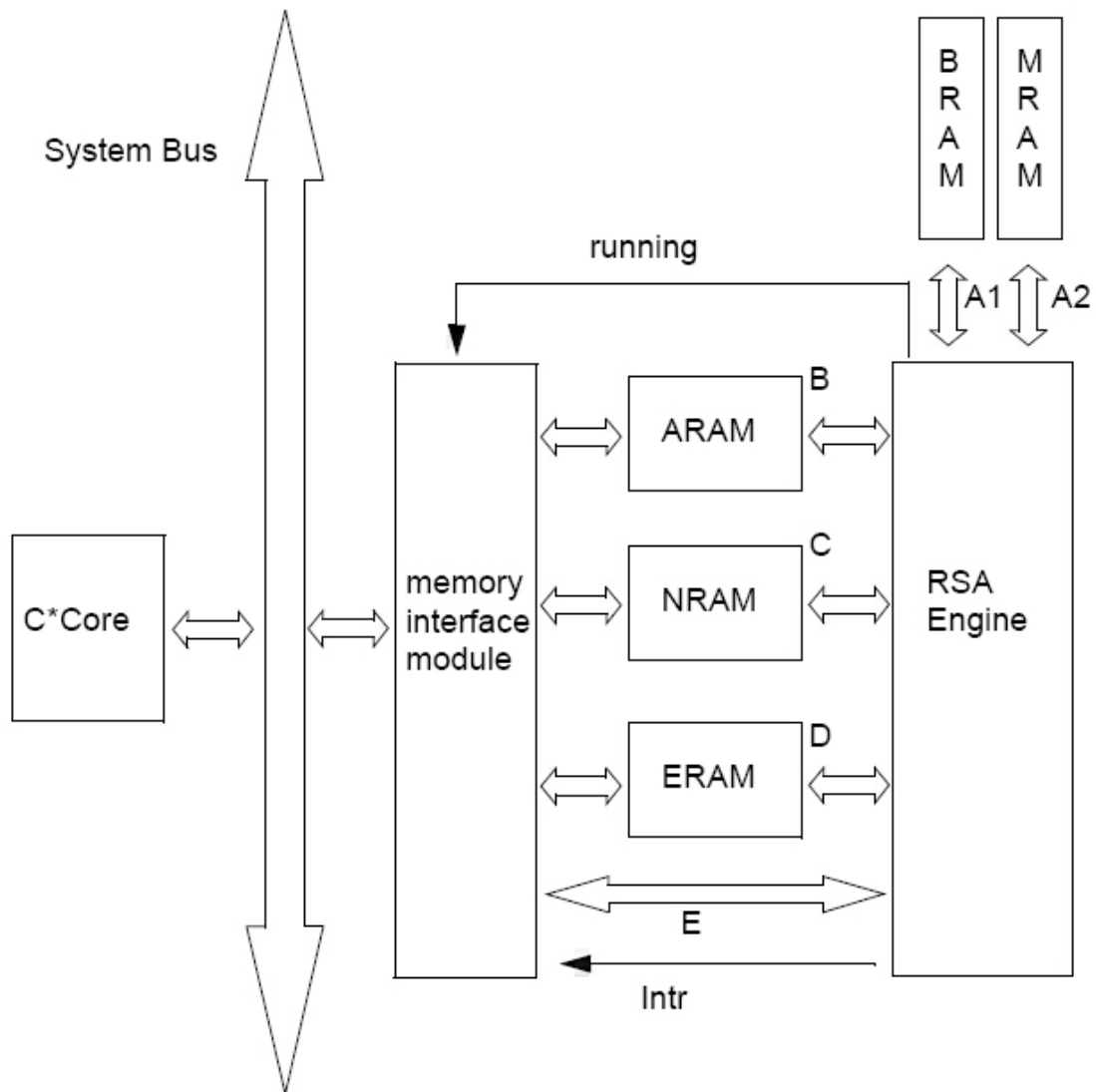


RSA Module

Summary

RSA is a module designed for implementation of RSA algorithm and it can accomplish 192/256/512/1024/2048 bits modular exponentiation/multiplication operation without using CRT.



RSA Block Diagram

Features

- Support public key cryptographic algorithms, such as RSA and ECC
- Support 192/256/512/1024/2048 bits RSA modular exponentiation/ multiplication calculation
- @80MHz:
 - 2048 bit RSA decryption 5 times per second
 - 2048 bit RSA encryption 900 times per second
 - 1024 bit RSA decryption 40 times per second
 - 1024 bit RSA encryption 3610 times per second

Low-Power Mode Operation

The RSA controller is not affected by any low-power modes. CPU can stop RSA by setting the corresponding module stop bit in Clock Module.

*To obtain more information about the RSA 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.*