

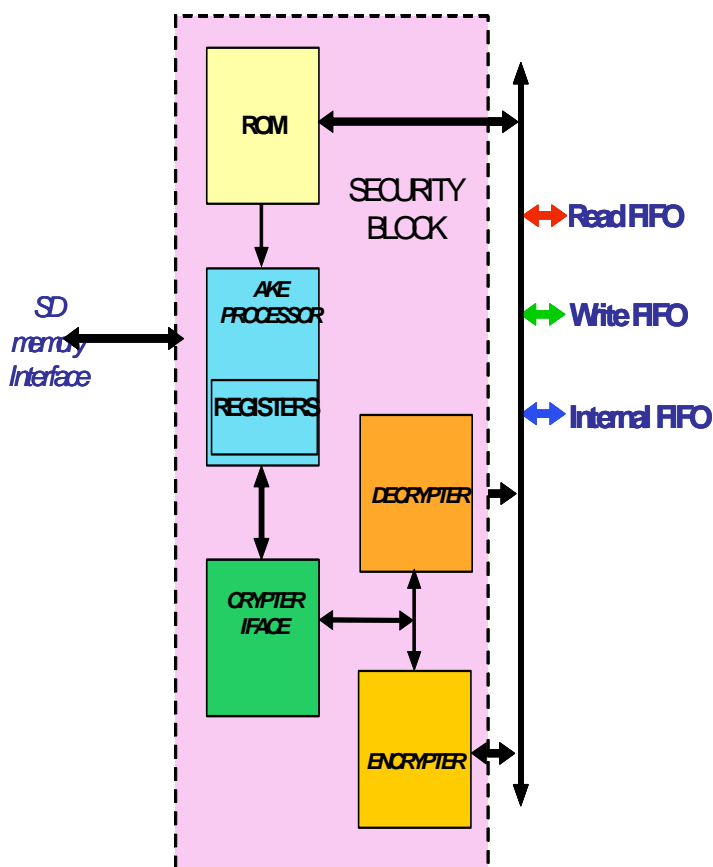
CPRM Security IP Core with AKE

Overview

Arasan_SD security with AKE IP is a standalone IP which could be integrated to any Device that requires Security implementation with Authentication algorithms that are compliant to CPRM specification. This product conforms to SD Memory Card Security Specification version 1.01 and to all the Cipher algorithms from 4C entity. Arasan SD security with AKE has the cipher algorithms implemented within it. Authentication processing is done using C2_G, C2_D and C2_E algorithms. User Area of the Flash can be accessed to read or write the encrypted data only upon a successful completion of Authentication. This algorithm needs a Session Key for performing encryption or decryption. C2_ECBC, C2_DCBC cipher algorithms are used for data encryption and decryption. This security block IP uses a clock of 100 MHz and it starts encryption and decryption process after receiving 8 bytes of data to have a good throughput.

Features

- *Complies with SD Memory Card Specifications Part3 : Security Specification Version 1.01
- *Complies with CPRM specification of SD memory Card Book common part Revision 0.96
- *Complies with C2 Block Cipher Specification Revision 1.0
- * Complies with SD Memory Card Specifications, Part2 : File System Specification, Version 2.00 Draft
- * Complies with SD Memory Card Specifications, Part1 : Physical Layer Specification, Version 2.00 Draft.
- *Supports serial peripheral interface [SPI], SD 1-bit and SD 4 -bit modes.
- *Supports Authentication in secured mode
- *Supports secure read, secure write, secured erase and secure delete
- *Block length or sector size of 512bytes is supported depending on the chosen storage device. Can be used for Updating MKBs.
- *Has a SD_memory controller interface for data reception and transmission in Different modes
- *Has a fifo interface to source and dump data into the flash or to the SD memory Controller interface.
- *Fully works on external clock of 100 MHZ
- *Design optimized for higher throughput.
- *Needs no extra SD clocks for the crypter algorithms to work on the data.



AKE Processor:

This block receives the random number1 and generates response using C2_G and C2_D algorithms. This block also sends challenge2 and verifies the response generated from the Host by again reworking on the response generation methods.

Session key calculations are done in this block and given as input to the crypter block for further processing data encryptions and decryptions.

Decrypter:

Using C2_DCBC algorithm as defined by 4C entity data decryption is done. This block handles the decryption of secure area data using session key. During a Secured Write transaction decrypter engine gets activated.

Encrypter:

Using C2_ECBC algorithm as defined by 4C entity data encryption is done. This block handles the encryption of secure area data using session key. During a Secured read transaction encrypter engine gets activated.

ROM :

Random Number generator Keys and Media Unique Key are stored in this read only Memory.

Registers:

Internal registers to store the Media Identifier, Device key sets etc are placed in this area.

Crypter Iface :

This is an interface between memory / flash controller and crypter. This block initiates encryption or decryption of data in fifo.

Deliverables:

- * RMM complaint VHDL or Verilog RTL
- * Test bench with compliance & synthesis scripts
- * Behavioural models
- * User manual
- * On-site support for customization

Custom Design Services:

Arasan Chip Systems is experienced in providing custom design services including logic, SoC, system and software designs.

Data Sheet Links: www.arasan.com

For a complete directory of Arasan IPs, please visit: www.arasan.com



Arasan Chip Systems, Inc.

1150 N. First St. Suite #211
San Jose CA 95112
Phone: 408-282-1600
Fax: 408-282-7800
Email: sales@arasan.com
www.arasan.com