Advanced Computing

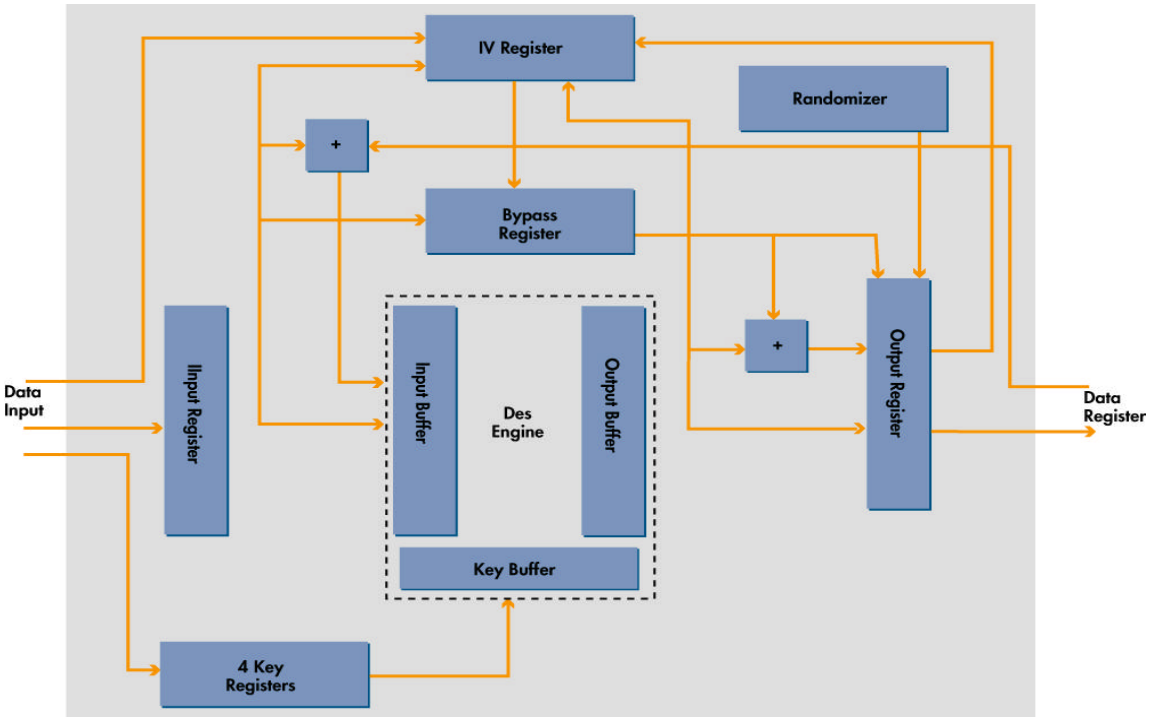
VMS110

16-Bit DES Coprocessor

OVERVIEW

The VMS110 is a powerful cryptographic chip designed for system flexibility to ease secure system implementations. VLSI provides the user a solution for applications such as cable access control and protection, offering a complete security solution for the security conscious designer.
The VMS110 is a high-speed ciphering engine that supports the Data Encryption Standard (DES) algorithm as specified by the National Institute of Standards and Technology Federal Information Processing Standards Publication #46-2 (FIPS PUB 46-2).
The VMS110 supports single DES Electronic Code Book and Cipher Block Chaining encryption/decryption.
The VMS110 uses a 16-bit bi-directional data bus and appears as a 16-bit peripheral to the host processor.
A 5-bit address field is used as the command input and control/status pins are available for host processor control and communication. The VMS 110 is a fully static design and supports clock rates up to 40 Mhz. Pipelined encryption/decryption for continuous blocks of data is implemented for both ECB and CBC modes. The VMS110 will complete an ECB mode in 8-clock cycles. The VMS110 also supports a bypass mode (plain data in with plain data out or cipher data in with cipher data out) which is cycle consistent with the equivalent encryption/ decryption mode.
Two 8-bit status and mode registers are present for current status and configuration/control of the VMS110. The MODE register is used select encrypt/decrypt modes and key usage. The STATUS/CONFIGURATION register is used to update the processor on the current state of the VMS110, set bypass mode, or select the ciphering operational mode; Electronic Codebook or Cipher Block Chaining.
The VMS110 key Cache consists of (4) 56-bit write only registers which allow for high speed key context switching. This multi-key cache will facilitate Single DES operations.
The VMS110 also includes VLSI Technology's digital non-deterministic randomizer (patent pending) for Initialization Vector (IV) and key generation, and random number seeding. Random bits are generated at greater than or equal to 1 Mbits/s. The randomizer does not require an external seed. The host processor can request and read a random 64-bit read/write status, input control, and read/write data. The host processor reads, writes, and configures the VMS110 via a 5-bit address field that is decoded by the VMS110 state machine and decoding logic. The VMS110 is memory mapped into the address space. The address command

Block Diagram



set includes reading the status, writing mode registers, loading cryptographic Keys, and loading and unloading plain and cipher data.
Once the VMS110 is setup, the VMS110 will automatically start a cipher process after the last 16-bit Least Significant Word (LSWord) is written. A start signal is not required to start the cipher process.

FEATURES

- Implements FIPS-PUB 46-2 Data Encryption Standard (8-cycle DES)
- Supports Single DES Electronic Codebook (ECB) and Cipher-Block-Chaining (CBC)
- Programmable Bypass Mode
- 16 Bit Bi-directional DATA I/O Port
- Simple register based control
- Clock rate up to 40 Mhz
- Data Throughput up to 35 M Bytes/s in Pipelined mode
- Built-in non-deterministic randomizer
- Built-in 4 Key Cache for high speed cryptographic context switching
- Implemented in low power CMOS technology
- Validated and certified by the National Institute of Standards and Technology

APPLICATION

Typical Applications and markets for the VMS110 and variants as follows:

- High Speed Cable Modems
- Embed into PC market to vend software and protect software privacy
- Electronic commerce for MTA or other financial applications
- Network Security: ATM, Ethernet, Internet, etc.
- High speed secure communication in general

SPECIFICATIONS

Export Control

This product is subject to U.S. Department of State regulations. Written U . S. Government approval is required prior to export.

Package

- 44-pin PLCC (Plastic Leadless Chip Carrier)

Recommended AC Operating Conditions

- Operating frequency range: 0 to 40 Mhz

Recommended DC Operating Conditions

- Supply Voltage (VDD): 5.0Vdc +/- 5%
- Input Signal Levels (5V dc):
  - VIH: 2.4 Vdc min., VDD max.
  - VIL: 0.0 V min., 0.8V max.
- Output Signal Levels (5V dc):
  - VOL: 0.3 VDD
  - VOH: 0.7 V min., VDD max.

Temperature Range

- 0 to 70° C

Storage Temperature

- -65° to +80° C

Device Evaluation Kit

An Evaluation Kit for the VMS110 is available to help customers understand the operation of the device. The evaluation kit is hosted on the ISA bus and consists of the following:

- PC Adapter Card
- Evaluation Program
- Users Guide
- Source Code and Associated Files

The PC adapter card fits into any 16-bit ISA bus slot of any IBM-compatible computer. With the evaluation program, users can download their own code and verify results. The program demonstrates features of the part and can, in fact, be used to sencrypt or decrypt files.

Ordering Information

- VMS110-EVAL: Evaluation Kit as listed above.
- VMS110: Packaged Unit (44 PLCC).

VLSI Technology

VLSI Technology, Inc.
1109 McKay Drive
San Jose, CA 95131