GENERAL DESCRIPTION

The **SGCIPH60** is one of STARGATE's **CIPHERTIME®** cores supporting the Advanced Encryption Standard (AES) (Rijndael). The Federal Information Processing Standard (FIPS) approved the Advanced Encryption Standard (FIPS-197) in the summer of 2001 and it is believed that it will become the encryption technology standard for the internet, wireless communications, and many other areas that require security The **SGCIPH60** is our high speed cipher core and is ideally suited for core network ASIC's requiring OC-48 grade speeds or more. The **SGCIPH60** can process data at 12.8 Gbps when implemented in 100MHz technology and can perform encryption as well as decryption. Blocks to be encrypted and decrypted may be interleaved on 128-bit block boundaries. ECB, CBC, OFB, CFB, and TIMER modes are supported.

FEATURES

- 12.8 Gbps at 100MHz/256-bit key/CBC, CFB, OFB, TMR
- 51.2 Gbps at 400MHz/256-bit key/ECB
- 14 Stage Pipeline/Caches
- Fully compliant with FIPS-197
- 400K gates (2-input Nand) + SSRAM + SROM
- 128, 192, and 256-bit keys
- Encryption and Decryption
- ECB, CBC, CFB, OFB, and TIMER mode support
- Separate Input, Output, Key, and Control Interface
- Key RAM for storing expanded encrypt/decrypt key
- 128-bit Input and Output Buffers
- Input and Output interface throttling

APPLICATIONS

- Secure Satellite Communications
- VPN Security
- Storage Area Networks
- Routers and Gateways
- Secure Telephony
- Secure Financial Transactions
- Secure Video

CORE INTEGRATION

The **SGCIPH60** core is fully synchronous, single positive edge triggered, and all Input and Output signals are registered insuring minimum delays across core boundaries. The **SGCIPH60** core requires 224 (512x8) synchronous ROM image used for Sbox and inverse Sbox table and 14 (16x128) SSRAM used for Expanded Encrypt/Decrypt Key storage.

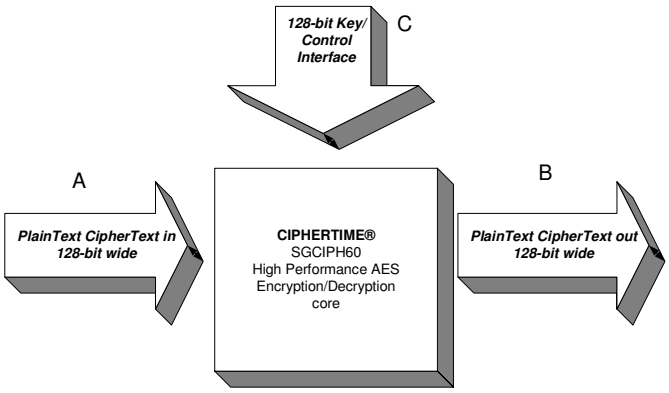

Figure 1.

INTERFACE DESCRIPTION

Figure 1. illustrates a block level view of the cipher and three interfaces used for connecting to other cores in the ASIC. The cipher operates on up to 14 separate blocks of data at the same time hence. Interface A, B, and C, are 128-bits wide. Interface A and B are used to connect to the high-speed or wire-speed data paths. During encryption, plaintext data is placed on input bus A and is then presented on output bus B after encryption is complete. During decryption, ciphertext data is placed on input bus A and then presented on output bus B after decryption is complete.

In order to obtain the ciphers maximum rated throughput, the input and output buffers must be serviced in time. Both input and output interface include control signals that are used to throttle the cipher. The purpose for throttling the cipher is to insure that input data is not overwritten and output data is not lost. Deeper FIFO's can easily be added to the input and output to accommodate systems with higher and unpredictable service latencies.

Interface C is used to control the cipher. The cipher can be started, stopped, reset, and key sizes can be programmed using this interface. Interface C is also used to download the key schedule to the key memory. The host processor must expand the key for both encryption and decryption and load the key schedule into this memory before starting the cipher.

PERFORMANCE

The **SGCIPH60** core is carefully coded and pipe-balanced to insure excellent synthesis results. New FSM design methods incorporated improve speed performance. Table 1. illustrates throughput obtained at various clock speeds and key sizes. Expected clock speed targets for Xilinx (Virtex-2/E) and ALTERA (APEX, Stratix) FPGA's should be around 100-150 MHz and ASIC technologies of .18-.12um should reach 200-400 MHz respectfully. At 400 MHz the **SGCIPH60** will process data at over 51.2 Gbps when multiplexing 14 separate streams. A stream is considered as a continuous set of blocks using the same key and any single mode. A single stream using CBC, CFB, OFB, or TIMER mode using a 128-bit key can obtain a maximum throughput of 5.12Gbps. A single stream using strictly ECB mode using a 128-bit key can obtain a maximum throughput of 51.2Gbps. Throughput performance can only be maintained only if input buffers are kept full and output buffers are kept empty. The **SGCIPH60** Input and output buffer service time is 1 cycle.

MHz	Key Size	Gbps
100	128	12.80
	192	12.80
	256	12.80
150	128	19.20
	192	19.20
	256	19.20
200	128	25.60
	192	25.60
	256	25.60
250	128	32.00
	192	32.00
	256	32.00
300	128	38.40
	192	38.40
	256	38.40
350	128	44.80
	192	44.80
	256	44.80
400	128	51.20
	192	51.20
	256	51.20

NOTE: Throughput performance can only be maintained if the input buffer is kept full and the output buffer is kept empty.

Table 1.

For more information on STARGATE products, please visit our web site at www.stargatesemiconductor.com or send us an E-mail at sales@stargatesemiconductor.com.

STARGATE Semiconductor, Inc.

STARGATE Semiconductor, Inc
One Burlington Business Center
67 South Bedford Street, Suite 400W
Burlington, MA 01803 USA
Tel (781) 229 - 5872
Fax (617) 472 - 3364
www.stargatesemiconductor.com