GENERAL DESCRIPTION

The **SGCIPH40** 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 **SGCIPH40** is our medium speed cipher core and is ideally suited for edge network ASIC's requiring OC-48 grade speeds or less. The **SGCIPH40** can process data at 2.9Gbps when implemented in 250MHz 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, and Timer modes are supported and newer cores introduced later this year will support all modes.

FEATURES

- 2.9 Gbps throughput at 250MHz/128-bit key
- 4.64 Gbps throughput at 400MHz/128-bit key
- Fully compliant with FIPS-197
- 30K gates (2-input Nand) + SSRAM + SROM
- 128, 192, and 256-bit keys
- Encryption and Decryption
- ECB, CBC, and TIMER modes
- Separate Input, Output, and Key/Control Interfaces
- Key RAM for storing expanded encrypt/decrypt key
- 128-bit Input and Output Buffers
- Input and Output interface throttling

APPLICATIONS

- Wireless Communications
- VPN Security
- Storage Area Networks
- Routers /Gateways
- Secure Telephony
- Secure Financial Transactions
- Secure Video

CORE INTEGRATION

The **SGCIPH40** core is fully synchronous, single positive edge triggered, and all Input and Output signals are registered insuring minimum delays across core boundaries. The **SGCIPH40** core requires 16 (512x8) separate synchronous ROM images used for Sbox and inverse Sbox Tables and 1 (16x128) SSRAM used for Expanded Encrypt/Decrypt Key storage.

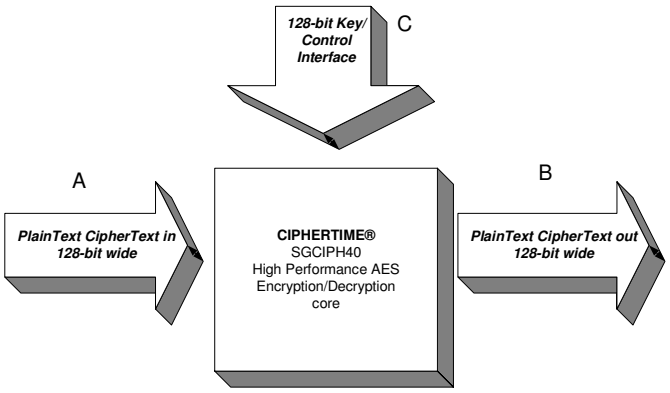

Figure 1.

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 a single block of data at a time hence the name "block cipher". Interface A and B are 128-bits wide and 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. The input buffer needs a new word written to it every 11, 13, or 15 clock cycles depending on what key size is used, and if not serviced in time, the cipher will wait until a new word is written. Likewise the output buffer needs to be read every 11, 13, or 15 clock cycles depending on what key size is used, and if not serviced in time, the cipher will wait until the date is read.

Both input and output interface include control signals that are used to throttle the cipher. The purpose for throttling 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.

TIMING

Figure 2. depicts a timing diagram for the Host interface. This interface is meant to be connected to a secure (FIPs boundary) subsystem which will handle key processing and expansion. Key information can only be written to the **SGCIPH40** through this interface and cannot be read back. The beginning of the timing diagram illustrates a reset cycle. WE_KEY, WE_IVCNTR, and WE_CTRL, signals should all be kept low during this time. The "a" shown at the top of the reset cycle in the timing diagram denote inserted wait states which should be at least one cycle as a minimum and may be an infinite number of cycles as a maximum. Following is a "b" wait cycle which denote that any number of wait states from 0 to infinity may be inserted. Following that are 5 write cycles to Key Memory, a write cycle to the IV Counter, and a write cycle to the Control Register. The "b" wait cycles are shown randomly about the timing diagram for illustration purposes and can be ignored if not applicable.

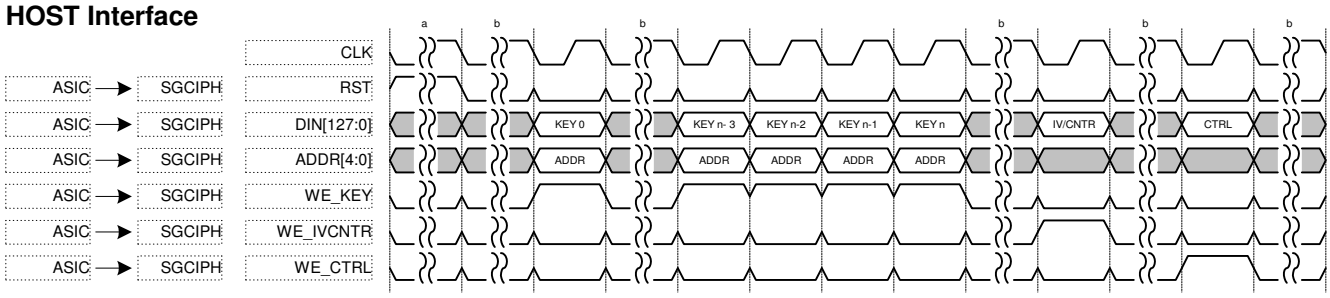

Figure 2.

Figure 3. Illustrates TXT input interface timing to the cipher. During encryption plaintext (PT) data is placed on the IN_DAT[127:0] signals and during decryption ciphertext (CT) data is placed on the IN_DAT[127:0] signals. The ASIC that passes PT or CT data to the input of the SGCIPH40 is considered an upstream device. The IN_RDY signal is used to indicate to the upstream device that the SGCIPH40 is ready to receive a block of data. The upstream device responds by presenting data on the IN_DAT[127:0] signals and asserting the IN_VALID signal indicating valid PT or CT is available. The SGCIPH40 indicates to the upstream device that it has latched in the data by deasserting IN_RDY. The "a"s shown along the top of the timing diagram denote inserted wait states which should be at least one cycle as a minimum and may be an infinite number of cycles as a maximum.

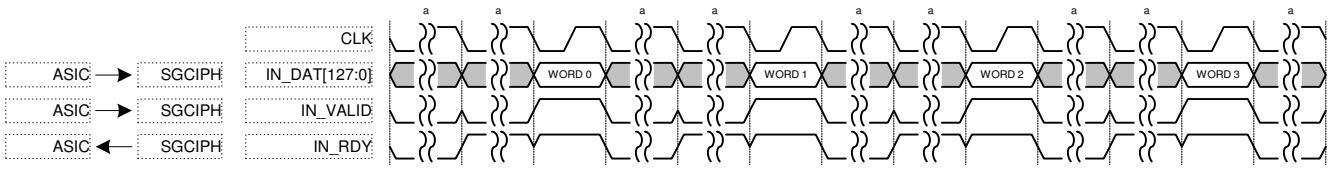

Figure 3.

Figure 4. Illustrates TXT output interface timing from the cipher. After encryption ciphertext (CT) data is placed on the OUT_DAT[127:0] signals or after decryption plaintext (PT) data is placed on the OUT_DAT[127:0] signals. The ASIC that receives PT or CT data from the output of the SGCIPH40 is considered a downstream device. The OUT_RDY signal is used to indicate to the SGCIPH40 that the downstream device is ready to receive data. The SGCIPH40 responds by presenting PT or CT data on the OUT_DAT[127:0] signals and asserting the OUT_VALID signal indicating valid data. The downstream device stream indicates to the SGCIPH40 that it has latched in the data by deasserting OUT_RDY. The "a"s shown along the top of the timing diagram denote inserted wait states which should be at least one cycle as a minimum and may be an infinite number of cycles as a maximum.

TXT OUTPUT Interface

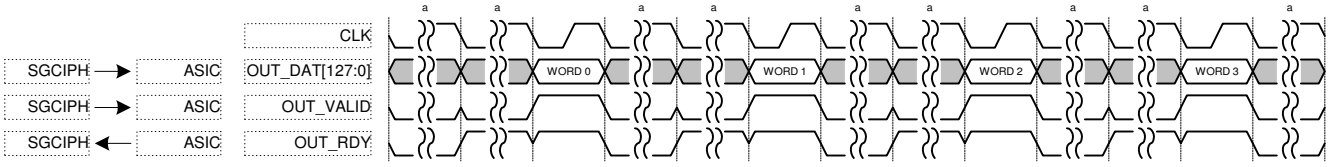

Figure 4.

PERFORMANCE

The **SGCIPH40** 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 **SGCIPH40** will process data at over 4.64 Gbps. Input and output buffer service time for 128, 192, and 256, bit keys are 11, 13, and 15 clocks cycles respectfully.

MHz	Key Size	Mbps
100	**128**	1163.64
	192	984.62
	256	853.33
150	**128**	1745.45
	192	1476.92
	256	1280.00
200	**128**	2327.27
	192	1969.23
	256	1706.67
250	**128**	2909.09
	192	2461.54
	256	2133.33
300	**128**	3490.91
	192	2953.85
	256	2560.00
350	**128**	4072.73
	192	3446.15
	256	2986.67
400	**128**	4654.55
	192	3938.46
	256	3413.33

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
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