GENERAL DESCRIPTION

The **SGCIPH20** 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 **SGCIPH20** is our low speed cipher core and is ideally suited for wireless applications. The **SGCIPH20** can process data at 73Mbps 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, and Timer modes are supported.

FEATURES

- 73 Mbps throughput at 100MHz/128-bit key
- 290 Mbps throughput at 400MHz/128-bit key
- Fully compliant with FIPS-197
- 8K 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, 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 802.11A/B
- VPN Security
- Storage Area Networks
- Routers and Gateways
- Secure Telephony
- Secure Financial Transactions
- Secure Video

CORE INTEGRATION

The **SGCIPH20** core is fully synchronous, single positive edge triggered, and all Input and Output signals are registered insuring minimum delays across core boundaries. The **SGCIPH20** core requires 1 (512x8) synchronous ROM image used for Sbox and inverse Sbox table and 1 (16x128) SSRAM used for Expanded Encrypt/Decrypt Key storage.

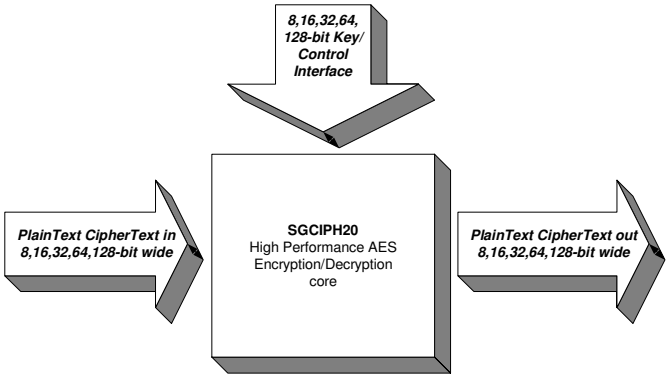

Figure 1.

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, B, and C, can be configured to be 8, 16, 32, 64, or 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. The input buffer needs a new word written every 176, 208, or 240 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 176, 208, or 240 clock cycles depending on what key size is used, and if not serviced in time, the cipher will wait until date is read .

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 **SGCIPH20** 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 **SGCIPH20** will process data at over 290 Mbps. Throughput performance can only be maintained if the input buffer is kept full and the output buffer is kept empty. Input and output buffer service time for 128, 192, and 256, bit keys are 176, 208, or 240 clock cycles respectfully.

MHz	Key Size	Mbps
100	**128**	72.73
	192	61.54
	256	53.33
150	**128**	109.09
	192	92.31
	256	80.00
200	**128**	145.45
	192	123.08
	256	106.67
250	**128**	181.82
	192	153.85
	256	133.33
300	**128**	218.18
	192	184.62
	256	160.00
350	**128**	254.55
	192	215.38
	256	186.67
400	**128**	290.91
	192	246.15
	256	213.33

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.

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