T7002 Bit Slice Multiplier and T7003 BSM Extender

Features

- Cascadable circuit design with 292 bits on T7002 and 298 bits on a T7003
- Microprocessor compatible interface
- Calculate A x B (mod M)
- Exponentiate $[B^{exp}]$ (mod M) under the control of a host processor
- Exponentiate at a rate of 27 ms for 512-bit operation
- Useful in public-key cryptography
- 1.5-micron CMOS design packaged in a standard 68-pin plastic leaded chip carrier

Description

The T7002 Bit Slice Multiplier (BSM) and T7003 BSM Extender form a cascadable circuit consisting of one T7002 chip followed by one or more T7003 chips. The T7002 BSM chip handles 292 multiplication bits, and each cascaded T7003 BSM Extender chip increases the bit length by 298 bits. The T7002 and T7003 circuit is designed as a microprocessor peripheral with only the T7002 chip interfacing with the host processor. Under the control of the processor, the T7002 and T7003 circuit may be used for calculating such mathematical equations as a modular exponentiation $[B^{exp}]$ (mod M). Since the T7002 and T7003 circuit performs modular operations, it is very useful in cryptographic applications. The T7002 and the T7003 chips are manufactured using 1.5-micron CMOS technology, require a 5 V supply, and are packaged in a 68-pin plastic leaded chip carrier.

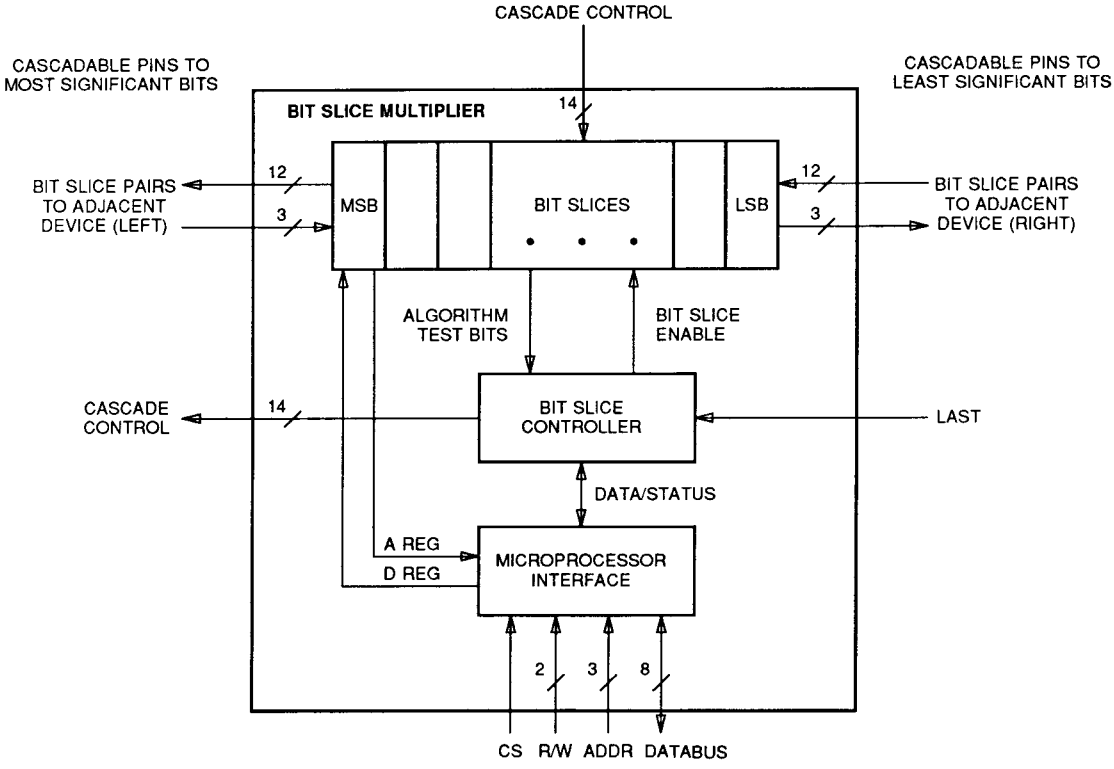

Figure 1. Block Diagram

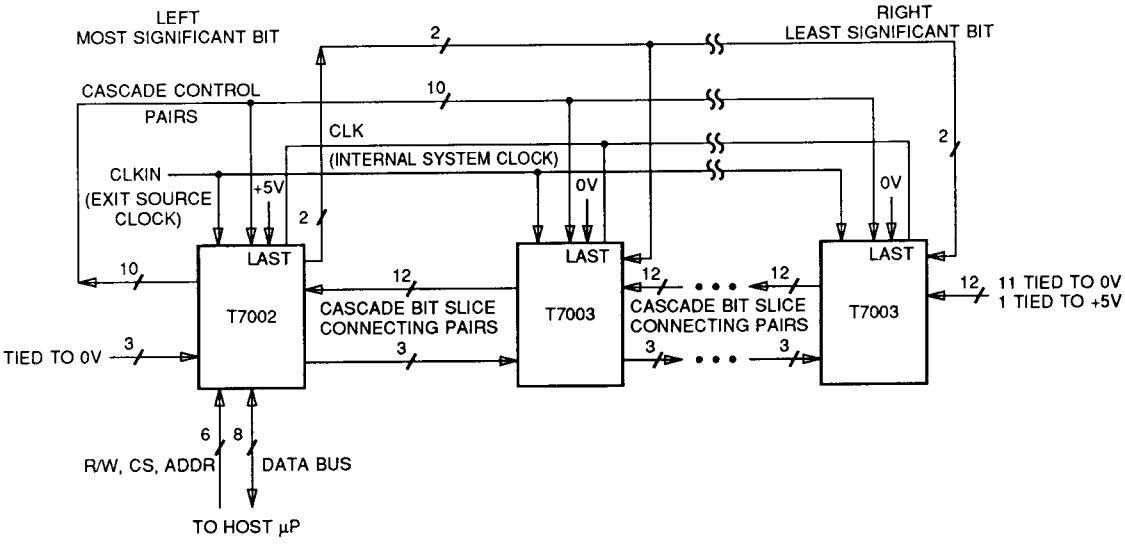

Figure 2. Cascade Block Diagram