MB9001C67

ULTRA SECURE CRYPTOGRAPHIC ACCELERATOR

1 Description

The Maple Instruments MB9001C67 offers unparalleled information security for the most critical applications. Using our trade secret cipher, it provides high-throughput confidentiality at low power.

2 Features

- 67-bit, military-grade encryption
- Proprietary cipher for increased security
  - No software implementations: impossible for hackers to reverse engineer
- Diverse applications
  - Copy protection for multimedia devices, game consoles
  - Authenticate commands for nuclear missile silos, military communications (see application note AN0237, "Using the MB90001C76 in the CRM 114 Discriminator")
  - Blockchain? I don't know what that is they told me to put it in here
- Simple operation: identical circuit for encryption and decryption

3 Package options

SOIC-8

4 Pinout and functions

[TOP VIEW]
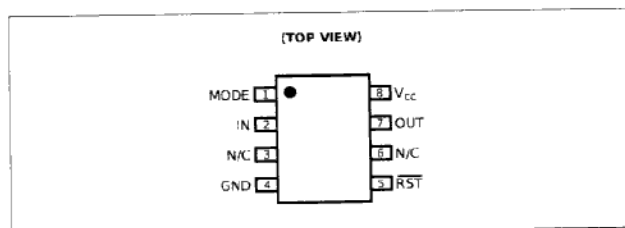
Pin		Description
1	MODE	Select loading new key/encryption
2	IN	Plaintext or ciphertext input
4	GND	Ground
5	RST	Reset, active low
7	OUT	Ciphertext or plaintext output
8	V$_{CC}$	Positive supply

5 Detailed description

To begin an encryption or decryption operation, hold the device in reset for at least one clock cycle. For the next 67 cycles, hold MODE high and provide the key (most significant bit first) on IN. The device will begin encrypting the plaintext or decrypting the ciphertext on the next cycle.
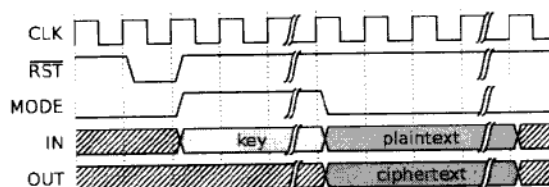
Note that the device begins encrypting immediately after loading the key. The sender and receiver must be synchronized in order to correctly encode and decode messages.

⚠ Never reuse the same key for different messages.

6 Encryption algorithm detail

The MB9001C67 encryption algorithm is based on a

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e

swag

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e

Figure 1: Internal structure ( )

(b)(3): 10 USC 130e

SSL added and removed here

(b)(3): 10 USC 130e

(b)(3): 10 USC 130e