Parallel Flash Security Silicon Sector Introduction

1. Introduction

Macronix offers parallel flash with a Security Silicon Sector region suitable for storing serial numbers or keys intended for security purposes. The Security Silicon Sector is 128 words of OTP (One Time Programmable) memory that resides outside the main memory array. It can be locked at the factory before shipping, or it can be locked later by the customer. Normally, this area is left unlocked when shipped and may be used as extra memory by the customer. This application note will explain how a customer can use this OTP area as extra memory.

2. Factory Locked and Customer Locked

By special order, customers may elect to have an ESN (Electronic Serial Number) programmed into the Security Silicon Sector and locked at the factory. If shipped unlocked, customers may use it as extra memory and lock it later.

2-1. Factory Locked

In a factory locked device, the Security Silicon Sector is programmed with a 16-Byte (8-Word) ESN and permanently locked at the factory before shipping to a customer. The Security Silicon Sector indicator bit will also be set to '1' indicating that the device was factory locked (see datasheet for read sequence required to check the status of Security Silicon Sector factory locked indicator bit Q7). Since this bit cannot be set by customers, cloning a factory locked device would be extremely difficult and provides a higher level of security. To order factory locked devices, please contact Macronix sales directly. Table 2-1 shows the Secured Silicon Sector structure and usage for factory and customer locked devices.

Table 2-1: Security Silicon Sector Structure

Secured Silicon Sector Density*[1]	Standard Factory Program/Locked	Express Flash Factory Program/Locked	Customer Program/Locked
8 Words	ESN	ESN or Determined by customer	Determined by customer
120 Words	Unavailable	Determined by customer	

Note:
1. See Macronix device datasheet for details of Secure Silicon Sector OTP address range.

Parallel Flash Security Silicon Sector Introduction

2-2. Customer Locked

In a customer locked device, the Security Silicon Sector indicator bit 'Q7' remains set to '0' indicating that it has not been programmed or protected at the factory. When the security locking feature is not required, the Security Silicon Sector is available for use as extra OTP memory space. Table 2-1 shows the Secured Silicon Sector structure space available for customer usage. In the MX29GLxxx series, the Security Silicon Sector area can be permanently locked by the customer by programming the OTP "Secured Silicon Sector Protection Bit" 'Q0' in the Lock Register to '0' (see Table 2-2). Users may refer to the Lock Register section in MX29GLxxx series datasheet for more detailed information.

The MX29LVxxx series do not have a Lock Register, but two alternate methods may be used to permanently lock the Security Silicon Sector. The first and preferred method does not require high voltage (Vhv[*1]) to be applied to specific pins while the second method does. Only the first method is described here.

To permanently protect the Security Silicon Sector without using Vhv, use the 3-cycle Enter Security Region command sequence followed by the Sector Group Protect algorithm (please refer to the datasheet for the algorithm's flow). The Sector Group Protect algorithm shows RESET# being set to Vhv, but it may be set to the normal input high level (Vih) when protecting the Security Silicon Sector. The Security Silicon Sector address used in the algorithm depends on the architecture of the device. For a top boot device, the sector address is all 1's. For a bottom boot device, the sector address is all 0's. Once the Security Sector is protected, there is NO way to unprotect it and its contents can no longer be altered.

Note:
1. High Voltage (Vhv) range is 9.5V ~ 10.5V. Any input greater than 10.5V may damage the flash device.

Table 2-2: Lock Register Bits

Q[15:3]	Q2	Q1	Q0
Don't Care	Password Protection Mode Lock Bit	Solid Protection Mode Lock Bit	Secured Silicon Sector Protection Bit [*1]

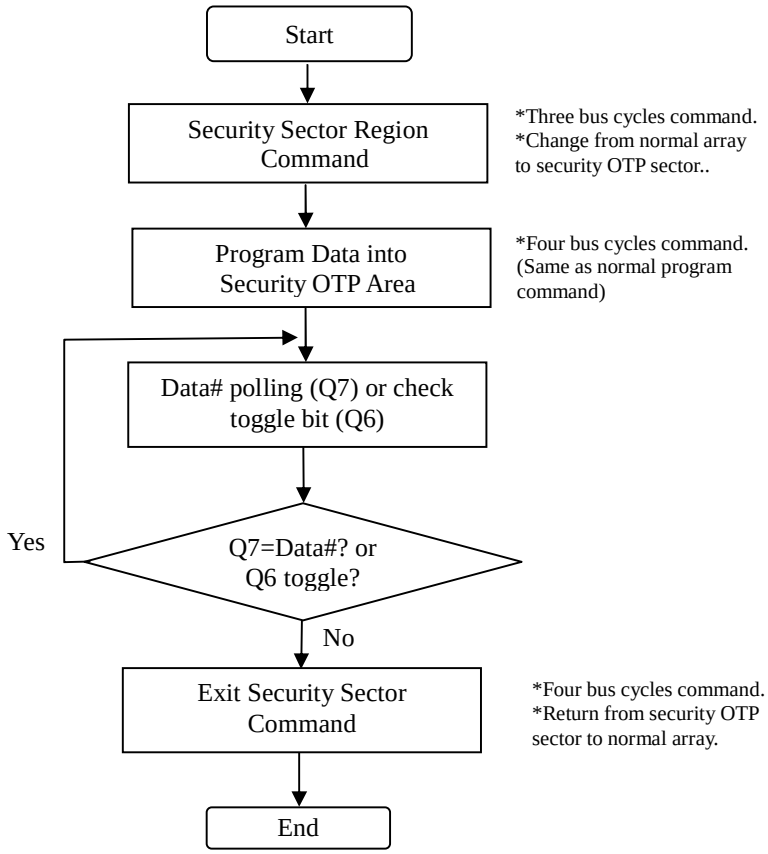
Note:
1. OTP Lock Register bit Q0=1 (default) indicates Secured Silicon Sector has not been locked by customer. See Macronix device datasheet for details on Programming and Reading Lock Register bits.

Parallel Flash Security Silicon Sector Introduction

3. Programming the Security Silicon Sector

When the security locking feature is not required, the Secure Silicon Sector region provides 128 words (256 bytes) of extra OTP memory space. To program the extra memory space, it must be entered by using the three bus cycle Security Sector Region command. After entering this region, the normal program instruction sequence may be used. The normal Data# polling and toggle bit methods are used to determine when the program operation has completed. Finally, the four bus cycle Exit Security Sector command is used to return to the main memory array. Figure 3-1 shows the flow.

Figure 3-1: Security Silicon Sector Program Flow

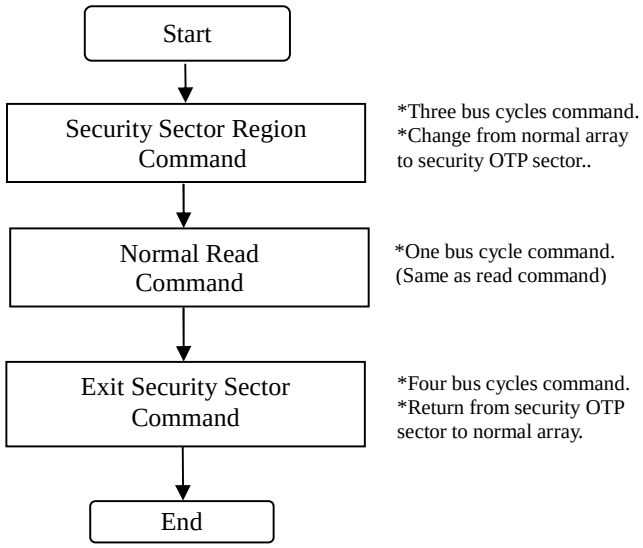


Parallel Flash Security Silicon Sector Introduction

4. Reading the Security Silicon Sector Region

To read the Security Silicon Sector, the three bus cycle Security Sector Region command must be executed first. The system may then use the normal read command to read the Security Silicon Sector content. When finished, the four bus cycle Exit Security Sector command is used to return to the normal "Read Main Memory Array" mode. Figure 4-1 shows the flow.

Figure 4-1: Security Silicon Sector Read Flow



5. Summary

The Security Silicon Sector provides an extra 128 words of OTP memory space. It can be locked by the factory before shipping or locked by the customer later. When the security locking feature is not required, it can be used by the application for data storage.

Parallel Flash Security Silicon Sector Introduction

6. Macronix Parallel Flash with Security OTP Region

The following Macronix parallel NOR Flash support the Security Silicon Sector OTP feature.

Table 6-1: Security Silicon Sector Support List

Density	Macronix Device
32Mb	MX29LV320E
	MX29GL320E
	MX29GA320E/GA321E
64Mb	MX29LV640E
	MX29GL640E
	MX29LA640E
	MX29GA640E/GA641E
128Mb	MX29GL128E/F
	MX29GA128E/GA129E
256Mb	MX29GL256E/F
	MX29GA256E/F
	MX29GA257E/F
512Mb	MX29GL512E/F
	MX29GA512F
1Gb	MX68GL1G0F

Parallel Flash Security Silicon Sector Introduction

7. References

Table 7-1 shows the datasheet versions used for comparison in this application note. For the most current, detailed specification, please refer to the Macronix website.

Table 7-1: Datasheet Version

Datasheet	Location	Data Issued	Version
MX29LV320E	Website	MAY 23, 2011	Rev 1.2
MX29GL320E	Website	DEC. 29, 2011	Rev 1.2
MX29GA320/321E	Website	APR. 14, 2011	Rev 1.1
MX29LV640E	Website	DEC. 27, 2011	Rev 1.7
MX29GL640E	Website	DEC. 27, 2011	Rev 1.4
MX29LA640E	Website	MAY 19, 2010	Rev. 1.3
MX29GA640/641E	Website	DEC. 11, 2009	Rev. 1.1
MX29GL128E	Website	DEC. 21, 2011	Rev. 1.5
MX29GL128F	Website	JUN. 28, 2012	Rev. 1.1
MX29GA128/129E	Website	AUG. 05, 2012	Rev. 1.0
MX29GA129/257E C/F	Website	NOV. 27, 2009	Rev. 1.0
MX29GA128/129/256/257E	Website	AUG. 05, 2011	Rev. 1.0
MX29GL256E	Website	JUL. 26, 2011	Rev. 1.4
MX29GL256F	Website	JAN. 12, 2012	Rev. 1.3
MX29GA256/257F	Website	AUG. 08, 2011	Rev. 1.0
MX29GL512E	Website	JUN. 16, 2011	Rev. 1.2
MX29GL512F	Website	JUL. 31, 2012	Rev. 1.4
MX29GA512F	Website	JUN. 28, 2012	Rev. 1.1
MX68GL1G0F	Website	JUL. 27, 2012	Rev. 1.0

8. Revision

Table 8-1: Revision History

Revision	Description	Date Issued
Rev. 1.0	Initial release	Dec. 11, 2012

Parallel Flash Security Silicon Sector Introduction

For the contact and order information, please visit Macronix's Web site at: http://www.macronix.com