Technical Note

MT25Q Protection and Security

Introduction

This technical note describes the implementation of the standard and advanced sector protection features for Micron's MT25Q Flash memory devices.

Standard protection features are legacy features and offer a simple but effective way to partially or totally protect the memory array against accidental or unwanted modification of its content.

Advanced sector protection offers additional levels of sector protection. It protects the memory from accidentally corrupting boot-up code and data stored, and it also prevents malicious attacks (e.g., from hackers) that could intentionally modify or corrupt the code or data stored in the memory.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.
Products and specifications discussed herein are for evaluation and reference purposes only and are subject to change by Micron without notice. Products are only warranted by Micron to meet Micron's production data sheet specifications. All information discussed herein is provided on an "as is" basis, without warranties of any kind.

Standard Protection

SPI Protocol Protection

SPI protocol protection is embedded into the SPI protocol itself and provides intrinsic protection against accidental modification of the memory array content:

- Power-On Reset and Internal Timer (^{t}VSL): Provides protection against inadvertent changes while the power supply is outside the operating specification. The memory interface does not execute the command unless it is input to the memory interface after power-on completes and after the power supply is set in the correct operating range.
- Write Enable Latch: All instructions that modify the array data or device configuration are executed only when the write enable latch bit in the status register is set (with the WRITE ENABLE instruction).
- Clock Count: All instructions that modify the array data or device configuration are verified to ensure the clock count is multiples of bytes before execution. If the command does not respect the specified frame, it is botched and not executed.

Legacy Nonvolatile Block Protect Bits Protection

Standard protection, based on the nonvolatile block protect bits (BP3, BP2, BP1, BP0) and the top/bottom bit of the status register, is a legacy feature and allows part of the memory (or even the entire array) to be configured as read-only. See the figure and table below for more details.

Figure 1: Status Register

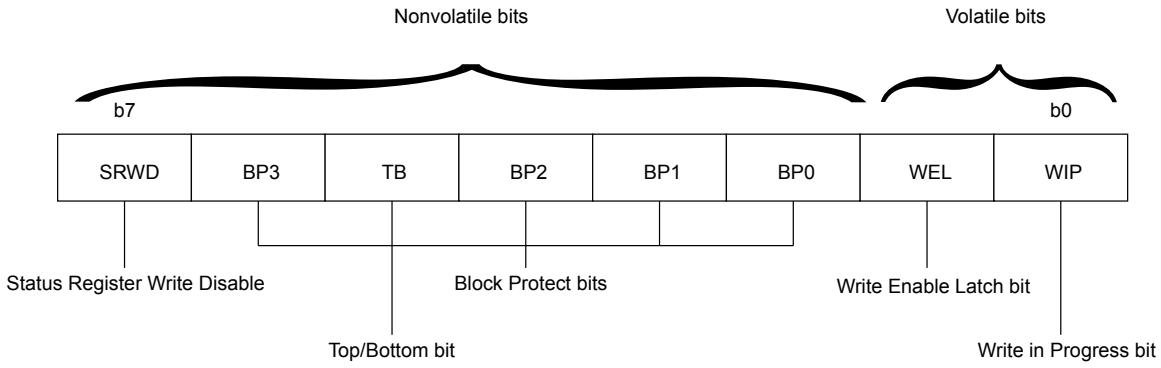


Table 1: Protected Area (64KB Sectors)

Note: The values shown are the numbers of protected blocks for 64KB sectors; each block has a dimension of 0.5Mb.

Status Register Content						Protected Sectors					
Top/ Bottom	BP3	BP2	BP1	BP0		64Mb	128Mb	256Mb	512Mb	1Gb	2Gb
0	0	0	0	0		None	None	None	None	None	None

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Table 1: Protected Area (64KB Sectors) (Continued)

Note: The values shown are the numbers of protected blocks for 64KB sectors; each block has a dimension of 0.5Mb.

Status Register Content						Protected Sectors					
Top/ Bottom	BP3	BP2	BP1	BP0		64Mb	128Mb	256Mb	512Mb	1Gb	2Gb
0	0	0	0	1		127	255	511	1023	2047	4095
0	0	0	1	0		127:126	255:254	511:510	1023:1022	2047:2046	4095:4094
0	0	0	1	1		127:124	255:252	511:509	1023:1021	2047:2045	4095:4092
0	0	1	0	0		127:120	255:248	511:504	1023:1016	2047:2040	4095:4088
0	0	1	0	1		127:112	255:240	511:496	1023:1008	2047:2032	4095:4080
0	0	1	1	0		127:96	255:224	511:480	1023:992	2047:2016	4095:4064
0	0	1	1	1		127:64	255:192	511:448	1023:960	2047:1984	4095:4032
0	1	0	0	0		All	255:128	511:384	1023:896	2047:1920	4095:3968
0	1	0	0	1		All	All	511:256	1023:768	2047:1792	4095:3840
0	1	0	1	0		All	All	All	1023:512	2047:1536	4095:3584
0	1	0	1	1		All	All	All	All	2047:1024	4095:3072
0	1	1	0	0		All	All	All	All	All	4095:2048
0	1	1	0	1		All	All	All	All	All	All
0	1	1	1	0		All	All	All	All	All	All
0	1	1	1	1		All	All	All	All	All	All
1	0	0	0	0		None	None	None	None	None	None
1	0	0	0	1		0	0	0	0:0	0	0
1	0	0	1	0		1:0	1:0	1:0	1:0	1:0	1:0
1	0	0	1	1		3:0	3:0	3:0	3:0	3:0	3:0
1	0	1	0	0		7:0	7:0	7:0	7:0	7:0	7:0
1	0	1	0	1		15:0	15:0	15:0	15:0	15:0	15:0
1	0	1	1	0		31:0	31:0	31:0	31:0	31:0	31:0
1	0	1	1	1		63:0	63:0	63:0	63:0	63:0	63:0
1	1	0	0	0		All	127:0	127:0	127:0	127:0	127:0
1	1	0	0	1		All	All	255:0	255:0	255:0	255:0
1	1	0	1	0		All	All	All	511:0	511:0	511:0
1	1	0	1	1		All	All	All	All	1023:0	1023:0
1	1	1	0	0		All	All	All	All	All	2047:0
1	1	1	0	1		All	All	All	All	All	All
1	1	1	1	0		All	All	All	All	All	All
1	1	1	1	1		All	All	All	All	All	All

The block protect bits (BP3, BP2, BP1, BP0) and the top/bottom bit of the status register bits can be read from or written to using READ STATUS REGISTER or WRITE STATUS REGISTER commands, respectively.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

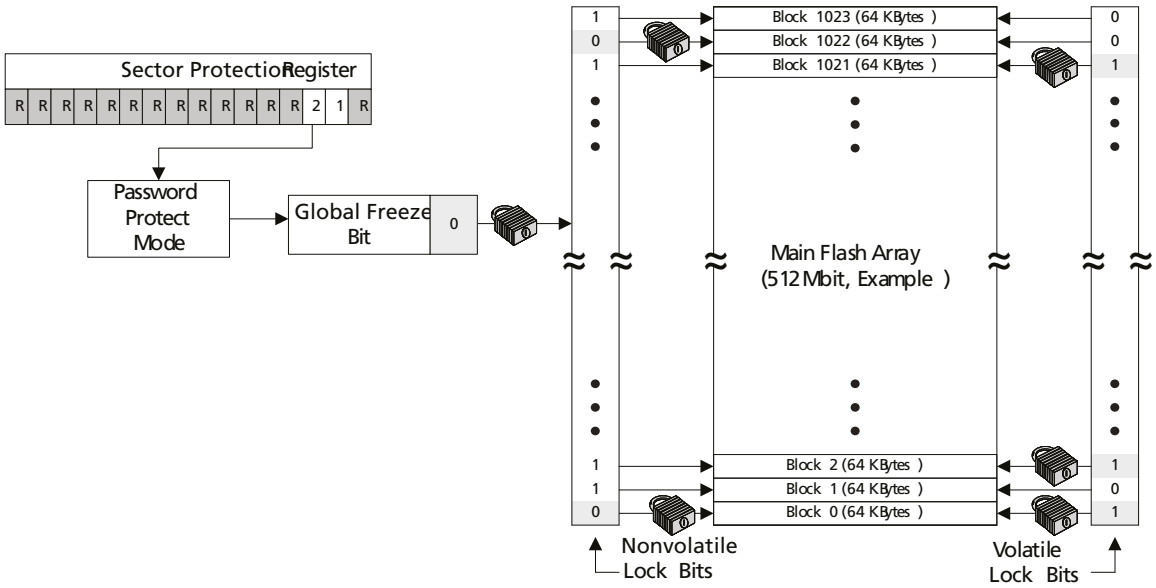
The WRITE STATUS REGISTER commands can also be used also to program the status register write enable/disable bit of the status register.

If the W# pin is held LOW (to V_{IL}) and the status register write enable/disable bit in the status register is set (i.e., programmed to 1), the status register nonvolatile bits become read-only and the WRITE STATUS REGISTER operation will not execute. The only way to exit this hardware-protected mode is to drive W# HIGH (to V_{IH}). This method offers a hardware means of protecting the array.

Advanced Sector Protection

Advanced sector protection offers volatile sector protection (through volatile lock bits) and nonvolatile sector protection (through nonvolatile lock bits) and also password protection over the nonvolatile lock bits. The following section describes the protections offered. See the figure below for an overview of the registers supporting advanced sector protection.

Figure 2: MT25Q Sector Locking Scheme



Volatile Lock Bit Security Register

One volatile lock bit register is associated with each sector of memory. It enables the sector to be locked, unlocked, or locked down with the WRITE VOLATILE LOCK BITS command, which executes only when sector lock-down (bit 1) is set to 0. Each register can be read with the READ VOLATILE LOCK BITS command. This register is compatible with and provides the same locking capability as the lock register in the legacy Micron N25Q Q-SPI NOR family.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Each volatile lock bit register has **two active bits**: the sector write lock bit (bit 0) and the sector write lock-down bit (bit 1). The other bits [7:2] of the volatile lock bit register are reserved.

- Bit 0: Sector Write Lock Bit. If the bit is set (1), the sector is write protected; instructions that attempt to change data in the sector are ignored and the protection fail bit in the flag status register is set. If the bit is reset (0), the sector is not protected.
- Bit 1: Sector Lock-Down Bit. When this bit is set (1), the write lock and write lock-down bits cannot be modified. A power cycle or reset operation is required to clear the lock-down bit. When the lock-down bit is reset (0), the write lock and lock-down bits can be changed.

On power-up and reset, the two active bits of the volatile lock bit register default to 00 (no lock-down, unlock).

Table 2: Volatile Lock Bit Register

Bit	Name	Settings	Description
7:2	Reserved	0	Bit values are 0.
1	Sector lock-down	0 = Lock-down disabled (default) 1 = Lock-down enabled	**Volatile bit:** Device always powers up with this bit set to 0 so that sector lock down and sector write lock bits can be set to 1. When this bit set to 1, neither of the two volatile lock bits can be written to until the next power cycle, or hardware or software reset.
0	Sector write lock	0 = Write lock disabled (default) 1 = Write lock enabled	**Volatile bit:** Device always powers up with this bit set to 0 so that PROGRAM and ERASE operations in this sector can be executed and sector content can be modified. When this bit is set to 1, PROGRAM and ERASE operations in this sector are not executed.

Nonvolatile Lock Bit Security Register

For nonvolatile sector locking, the lock bits are stored in flash cells within an erasable sector lock-bit array, hence, making this a nonvolatile locking scheme. An erased (i.e., FFh) nonvolatile lock register corresponds to an unlocked sector, and a programmed (i.e., 00h) nonvolatile lock register corresponds to a locked sector. One nonvolatile lock register is related to each sector. The nonvolatile lock registers are programmed individually by means of the WRITE NONVOLATILE LOCK BITS command but must be erased as a group using the ERASE NONVOLATILE LOCK BITS command. The content of the nonvolatile lock registers can be read out by using the READ NONVOLATILE LOCK BITS command.

Sector Protection Register

The sector protection register is used to enable different nonvolatile protection modes. It does not affect the volatile protection. By default, all devices from the factory will have the nonvolatile sector locking scheme enabled with sectors unlocked. Customers are required to activate the password, or persistent protect mode, and prevent it from future changes.

The desired protection mode is activated by setting one of the following sector protection register bits: Persistent protection mode lock bit (bit 1 of the sector protection register) and the password protection mode lock bit (bit 2 of the sector protection register). Programming the persistent protection mode lock bit or the password protection mode lock bit to 0 will permanently activate persistent protection or password protection, re-

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

spectively. These two bits are one-time programmable and nonvolatile. Once the protection mode has been programmed, it cannot be changed, and the device will permanently operate in the selected protection mode. Bits 2 and 1 of the sector protection register are one-time-programmable and mutually exclusive in that only one of them can be set to 0. It is recommended that one of the bits be set to 0 when first programming the device. In addition, it is recommended that the desired software protection mode be activated when first programming the device.

Table 3: Sector Protection Register

Bits	Name	Settings	Description	Notes
15:3	Reserved	1 = Default	–	
2	Password protection lock	1 = Disabled (default) 0 = Enabled	**Nonvolatile bit:** When set to 1, password protection is disabled. When set to 0, password protection is enabled permanently; the 64-bit password cannot be retrieved or reset.	1, 2
1	Sector protection lock	1 = Enabled, with password protection (default) 0 = Enabled, without password protection	**Nonvolatile bit:** When set to 1, nonvolatile lock bits can be set to lock/unlock their corresponding memory sectors; bit 2 can be set to 0 to permanently enable password protection. When set to 0, nonvolatile lock bits can be set to lock/unlock their corresponding memory sectors; bit 2 must remain set to 1 to permanently disable password protection.	1,3,4
0	Reserved	1 = Default	–	

Notes:
1. Bits 2 and 1 are user-configurable, one-time-programmable, and mutually exclusive in that only one of them can be set to 0. It is recommended that one of the bits be set to 0 when first programming the device.
2. The 64-bit password must be programmed and verified before this bit is set to 0 because after it is set, password changes are not allowed, thus providing protection from malicious software. When this bit is set to 0, a 64-bit password is required to reset the global freeze bit from 0 to 1. In addition, if the password is incorrect or lost, the global freeze bit can no longer be set and nonvolatile lock bits cannot be changed. (See the Sector and Password Protection figure and the Global Freeze Bit Definition table.)
3. Whether this bit is set to 1 or 0, it enables programming or erasing nonvolatile lock bits (which provide memory sector protection). The password protection bit must be set beforehand because setting this bit will either enable password protection permanently (bit 2 = 0) or disable password protection permanently (bit 1 = 0).
4. By default, all sectors are unlocked when the device is shipped from the factory. Sectors are locked, unlocked, read, or locked down as explained in the nonvolatile and Volatile Lock Bits table and the Volatile Lock Bit Register Bit Definitions table.

Global Freeze Bit

The global freeze bit is one volatile bit used to protect all nonvolatile lock register bits. The READ GLOBAL FREEZE BIT command enables reading this bit. Once the nonvolatile sector locking is complete, the WRITE GLOBAL FREEZE BIT command can be used to protect the nonvolatile lock register bits by clearing the global freeze bit to 0, which disables programming or erasing all of the nonvolatile lock register bits. See the table below.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Table 4: Global Freeze Bit

Bits	Name	Settings	Description
7:1	Reserved	0	Bit values are 0
0	Global freeze bit	1 = Disabled (default) 0 = Enabled	**Volatile bit:** When set to 1, all nonvolatile lock bits can be set to enable or disable locking their corresponding memory sectors. When set to 0, nonvolatile lock bits are protected from PROGRAM or ERASE commands. This bit should not be set to 0 until the nonvolatile lock bits are set.

Note: 1. The READ GLOBAL FREEZE BIT command enables reading this bit. When password protection is enabled, this bit is locked upon device power-up or reset. It cannot be changed without the password. After the password is entered, the UNLOCK PASSWORD command resets this bit to 1, enabling programming or erasing the nonvolatile lock bits. After the bits are changed, the WRITE GLOBAL FREEZE BIT command sets this bit to 0, protecting the nonvolatile lock bits from PROGRAM or ERASE operations.

Password Protection Mode

In password protection mode, the global freeze bit defaults to 0 on hardware reset or power-up, and all of the nonvolatile lock register bits are protected. The user must provide the password to set this bit to 1 in order to enable programming or to erase the nonvolatile lock register bits.

To set the memory in password protection mode, the following steps are required.

Prior to entering the password protection mode, it is necessary to set a 64-bit password using the WRITE PASSWORD command and then verify it using the READ PASSWORD command. Note:

- For the WRITE PASSWORD command, the 64-bit password data must be entered with least significant byte first, most significant bit of each byte first.
- For the READ PASSWORD command, the 64-bit password data is shifted out with the least significant byte first, most significant bit of each byte first. When read continuously, the device outputs the 64-bit data repeatedly.

The password protection mode is then activated by programming the password protection lock, i.e., bit 2 of the sector protection register is set to 0 (all remaining bits of the sector protection register must stay at 1). This operation is not reversible, and once bit 2 of the sector protection register is programmed, it cannot be erased. The device permanently remains in password protection mode, and the 64-bit password cannot be retrieved or reprogrammed (i.e., there is no means to verify the password after bit 2 of the sector protection register is set).

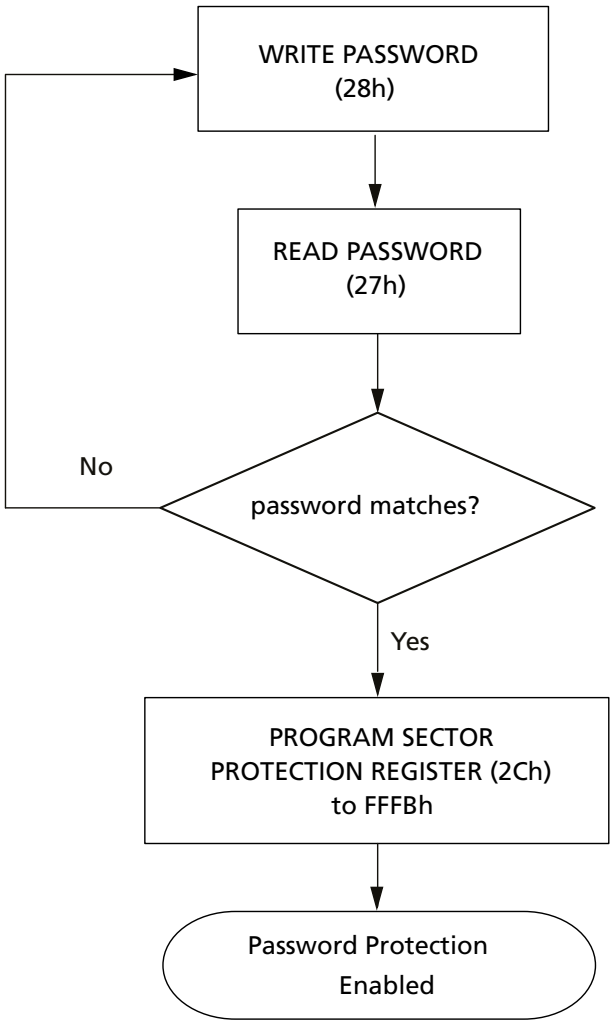
To program the sector protection register, the PROGRAM SECTOR PROTECTION command must be used. Note that the sector protection register is two data bytes in length. After the 8-bit instruction is shifted in, the 16-bit sector protection register contents are shifted in on the serial input, least significant byte first, most significant bit of each byte first.

Moreover, once the UNLOCK PASSWORD succeeds, the global freeze bit is set to 1 to allow nonvolatile lock bits to be changed. However, after issuing the WRITE NONVOLATILE LOCK BITS command or the ERASE NONVOLATILE LOCK BITS command, the device will not automatically revert to the password locked state (i.e., the global freeze bit

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

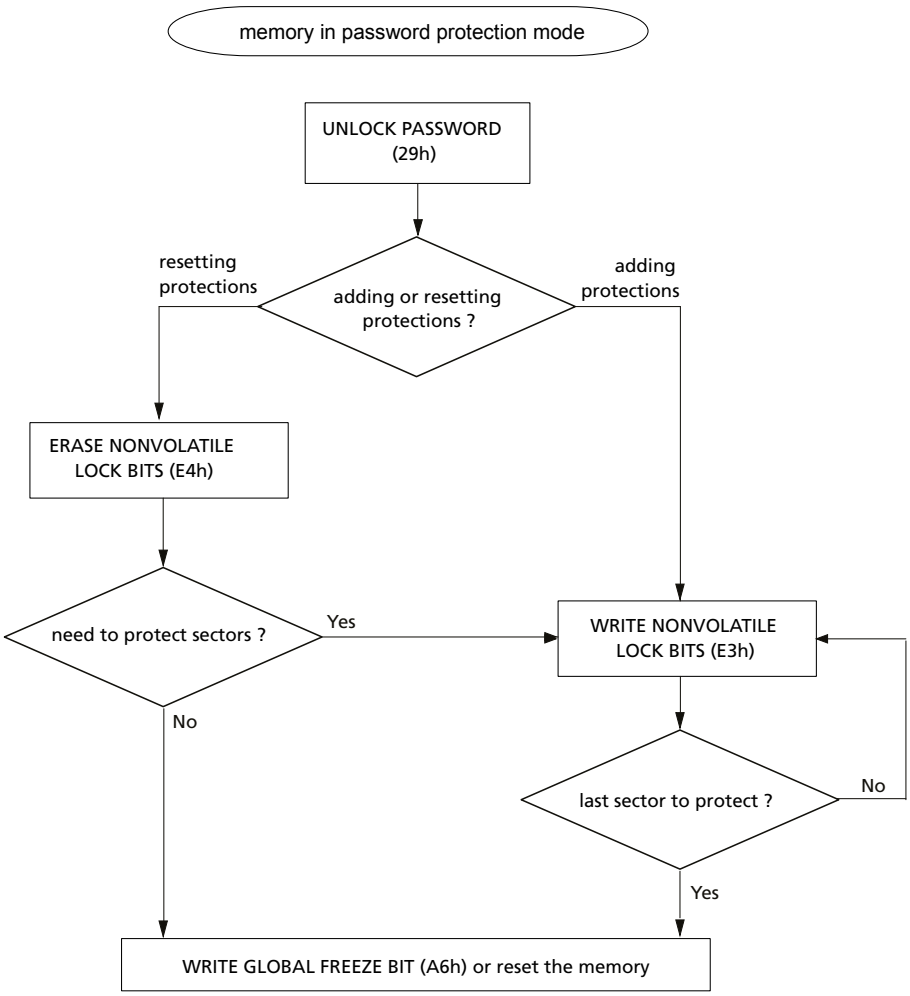
stays at 1), and a WRITE GLOBAL FREEZE BIT command can be issued to return the device to the password locked state.

Figure 3: Setting Password Protection Mode



Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Figure 4: Protecting and Unprotecting Sectors in Password Protection Mode



Persistent Protection Mode

In persistent protection mode, the global freeze bit defaults to 1 on hardware reset or power-up. The WRITE GLOBAL FREEZE BIT command clears this bit to 0, locks all non-volatile lock register bits to their current state, and requires a hardware reset to unlock. To set the memory in persistent protection mode, bit 1 of the sector protection register must be programmed to 0 using the PROGRAM SECTOR PROTECTION command. The sector protection register is two data bytes in length. After the 8-bit instruction shifts in, the 16-bit sector protection register contents are shifted in on the serial input, least significant byte first, most significant bit of each byte first. As reported previously, this operation is not reversible. If the user does not want to activate the password protection mode, it is strongly recommended that the persistent protection mode be explicitly activated to permanently disable password protection.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Figure 5: Protecting and Unprotecting Sectors in Persistent Protection Mode

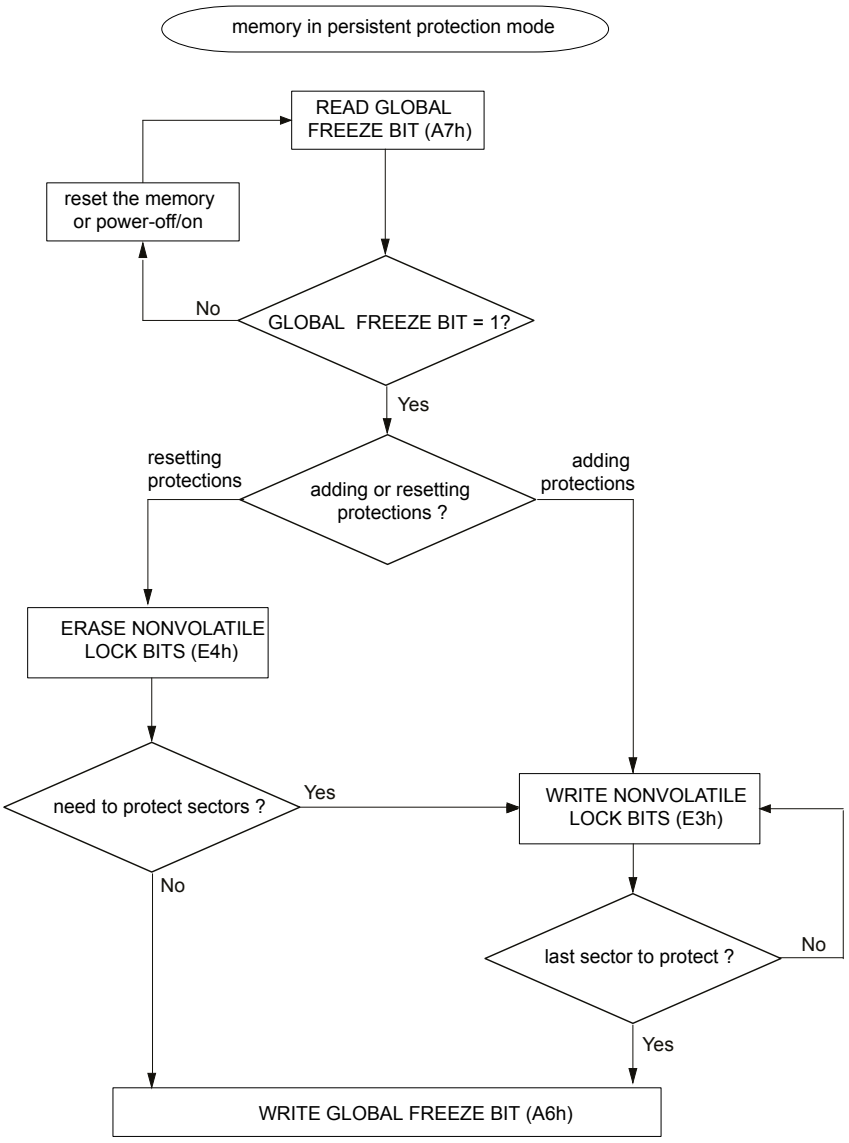


Table 5: Nonvolatile and Volatile Lock Bits Summary

Bit Details	Nonvolatile Lock Bit	Volatile Lock Bit
Description	Each sector of memory has one corresponding nonvolatile lock bit.	Each sector of memory has one corresponding volatile lock bit; this bit is the sector write lock bit described in the volatile lock bit register table.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Table 5: Nonvolatile and Volatile Lock Bits Summary (Continued)

Bit Details	Nonvolatile Lock Bit	Volatile Lock Bit
Function	When set to 0, locks and protects its corresponding memory sector from PROGRAM or ERASE operations. Because this bit is nonvolatile, the sector remains locked, with protection enabled, until the bit is cleared to 1.	When set to 1, locks and protects its corresponding memory sector from PROGRAM or ERASE operations. Because this bit is volatile, protection is temporary. The sector is unlocked, with protection disabled, upon device reset or power-down.
Settings	1 = Lock disabled 0 = Lock enabled	0 = Lock disabled 1 = Lock enabled
Enabling Protection	The bit is set to 0 by the WRITE NONVOLATILE LOCK BITS command, enabling protection for designated locked sectors. Programming a sector lock bit requires the typical byte programming time.	The bit is set to 1 by the WRITE VOLATILE LOCK BITS command, enabling protection for designated locked sectors.
Disabling Protection	All bits are cleared to 1 by the ERASE NONVOLATILE LOCK BITS command, unlocking and disabling protection for all sectors simultaneously. Erasing all sector lock bits requires typical sector erase time.	All bits are set to 0 upon reset or power-down, unlocking and disabling protection for all sectors.
Reading the Bit	Bits are read by the READ NONVOLATILE LOCK BITS command.	Bits are read by the READ VOLATILE LOCK BITS command.

Additional MT25Q Security Features

In addition to the sector protection features described previously, Micron's MT25Q family offers additional features that can be used to improve security:

- 17 Bytes for Unique ID (UID) code in the Device ID Data
- Dedicated 64-Byte OTP Area Outside Main Array

Device ID Data

- 1 byte for manufacturer identification (20h)
- 2 bytes for device identification (first byte for memory type, second byte for memory capacity)
- 17 bytes for unique ID (UID) code, of which 14 are factory programmed with a data string that is **unique and different for each part**

The device ID data shown in the tables below is read by the READ ID and MULTIPLE I/O READ ID operations.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Table 6: Device ID Data

Byte#	Name	Content Value	Assigned By
Manufacturer ID (1 byte total)			
1	Manufacturer ID (1 byte)	20h	JEDEC
Device ID (2 bytes total)			
2	Memory type (1 byte)	BAh = 3V	Manufacturer
		BBh = 1.8V	
3	Memory capacity (1 byte)	22h = 2Gb	
		21h = 1Gb	
		20h = 512Mb	
		19h = 256Mb	
		18h = 128Mb	
		17h = 64Mb	
Unique ID (17 bytes total)			
4	Indicates the number of remaining ID bytes (1 byte)	10h	Factory
5	Extended device ID (1 byte)	See Extended Device ID table	
6	Device configuration information (1 byte)	00h = Standard	
7:20	Customized factory data (14 bytes)	Unique ID code (UID)	

Table 7: Extended Device ID Data, First Byte

Bit 7	Bit 6	Bit 5[1]	Bit 4	Bit 3	Bit 2[2]	Bit 1	Bit 0
Reserved	Device generation 1 = 2nd generation	1 = Alternate BP scheme 0 = Standard BP scheme	Reserved	HOLD#/RESET#: 0 = HOLD 1 = RESET	Additional HW RESET#: 1 = Available 0 = Not available	Sector size: 00 = Uniform 64KB	

Notes:
1. For alternate BP scheme information, contact the factory.
2. Available for specific part numbers. See Part Number Ordering Information for details.

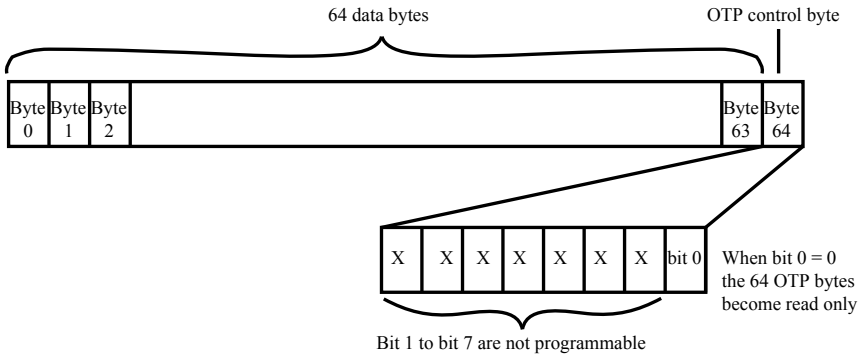
Dedicated 64-Byte OTP Area Outside Main Array

MT25Q devices include a 64-byte one-time-programmable (OTP) memory area that can be programmed and read through dedicated PROGRAM OTP ARRAY and READ OTP ARRAY commands.

These OTP bytes may be permanently locked by programming bit 0 of the 64th byte to 0 (see the figure below).

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Figure 6: One-Time Programmable (OTP) Area



Summary

This technical note provides an overview of the standard and advanced protection features, as well as basic security options, available on MT25Q devices for standard Micron part numbers. Users can choose the most appropriate way, based on their needs, to protect the boot-up code and data stored in the memory array and protect the data against accidental or malicious modifications.

Refer to Micron's MT25Q data sheets for more information.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.

Revision History

Rev. A – 12/2020

- Initial release

8000 S. Federal Way, P.O. Box 6, Boise, ID 83707-0006, Tel: 208-368-4000
www.micron.com/products/support Sales inquiries: 800-932-4992
Micron and the Micron logo are trademarks of Micron Technology, Inc.
All other trademarks are the property of their respective owners.

Micron Technology, Inc. reserves the right to change products or specifications without notice.
© 2020 Micron Technology, Inc. All rights reserved.