Block Locking Security Using OTP Registers

309044-01

Contents

Revision History

Date	Revision	Description
July 2009	001	Original version

1.0 Overview

The Numonyx™ P30 and P33 Flash Memory (65nm) feature enhanced security modes used to protect and secure the information stored in the flash Main Memory array. This document will explain how the standard One Time Programmable (OTP) Protection Registers may optionally be used to protect data in the Main Memory Array. For more information about Protection Register operation, please refer to the P30 or P33 datasheet.

The code and/or data within the flash Main Memory array may be optionally protected or secured as One Time programmable with the use of the Protection Registers. The Protection Registers are memory locations independent from the Main Memory array. By mapping the Protection Registers to control the Main Memory array as OTP, the Main Memory may be set to no longer allow programming or erasing; they can only be read. This feature is a special OTP protection feature and is different from the normal "block locking"of the Main Array. Information about "block locking"of the Main Array can be found in the P30 or P33 datasheet.

One Time Protection is available in 3 different customer ordered options - "standard", "simple" and "device" OTP. The first option, "standard OTP", does not allow any special OTP protection of the Main Memory array and is available in all Flash configurations. The second option, "simple OTP", allows up to 512K of Main Memory OTP protection. This option pre-defines 512K of the main array that includes the 4x32 KB parameter blocks ganged together as one block and the adjacent 3x128 KB main blocks. The third option, "device OTP", will allow protection of data in all of the Main Memory array blocks. All of these options are available for top or bottom boot devices.

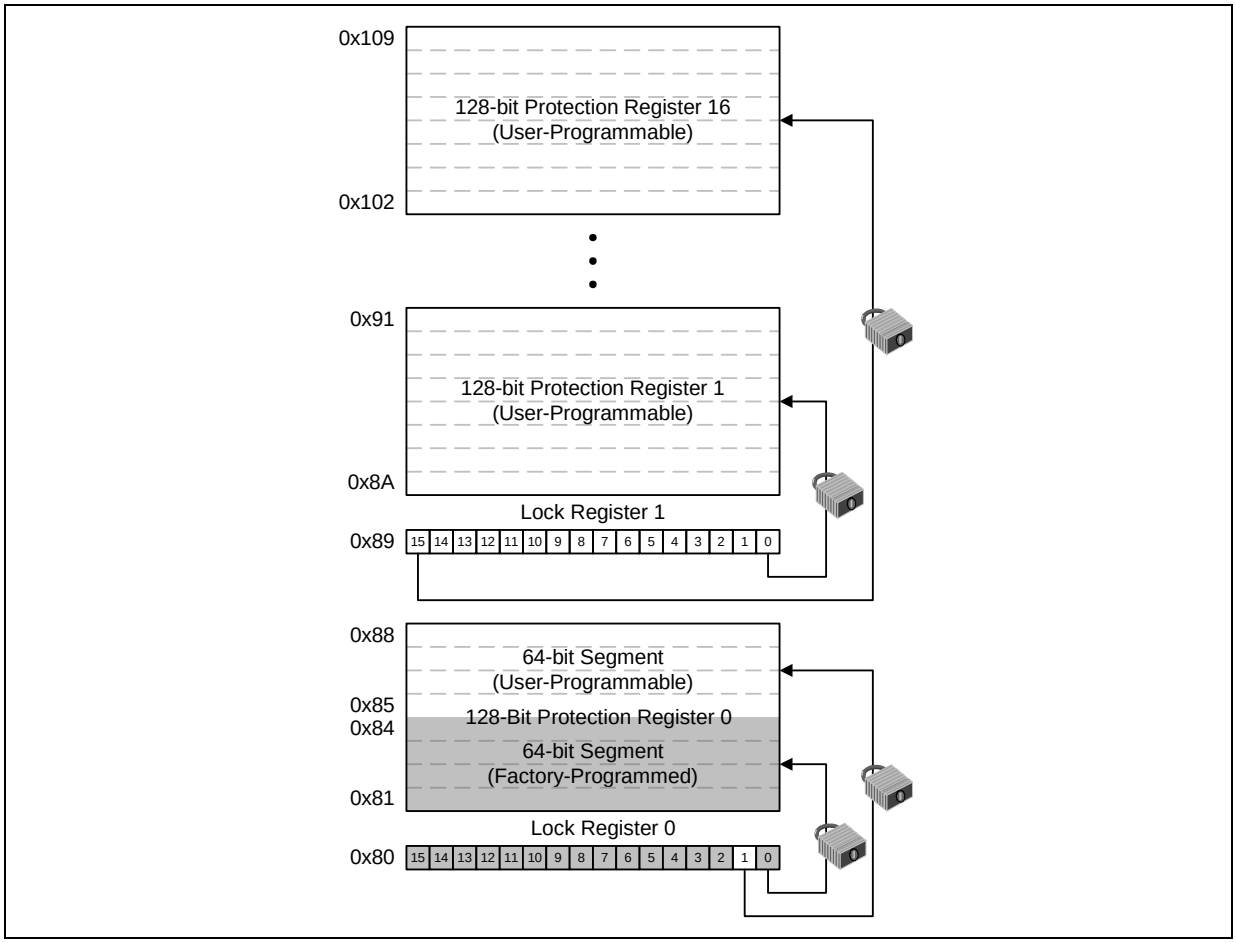
Note: For more information about the device refer to the Numonyx™ P30 and P33 Flash Memory (65nm) Datasheet.

2.0 "Standard" System Protection Registers

Every P30 and P33 contains seventeen 128-bit individually lockable Protection Registers that can increase system security or prevent device substitution by containing values that mate the flash component to the system's CPU or ASIC. See Table 1, "Read Identifier Table" on page 3. These Protection Registers are a part every P30 and P33 Flash component.

The first 128-bit Protection Register is comprised of two 64-bit (8-word) segments. The lower 64-bit segment is pre-programmed at the Numonyx factory with a unique 64-bit number. The other 64-bit segment, as well as the other sixteen 128-bit Protection Registers, are blank, and users can program these registers as needed. Once programmed, each customer segment can be further locked to prevent further programming. Refer to Figure 1, "Protection Register Map" on page 2.

Figure 1: Protection Register Map



2.1 Read Protection Register

The Read Identifier command allows protection register data to be read 16 bits at a time from addresses shown in Table 1, “Read Identifier Table” on page 3. To read the protection register, first issue the Read Device Identifier command to Device Base Address to place the device in the Read Device Identifier mode. Next, perform a read operation at the device’s base address plus the address offset corresponding to the register to be read. For example, the address offset for Lock Register 0 would be 0x80h as shown in Figure 1.

Table 1: Read Identifier Table

Item	Address	Data
Manufacturer Code	0x00	0089h
Device ID Code	0x01	ID
Block Lock Configuration: • Block Is Unlocked • Block Is Locked • Block Is not Locked-Down • Block Is Locked-Down	Block Base Address + 0x02	Lock Bit: DQ_0 = 0b0 DQ_0 = 0b1 DQ_1 = 0b0 DQ_1 = 0b1
Read Configuration Register	0x05	RCR Contents
Lock Register 0	0x80	PR-LK0
64-bit Factory-Programmed Protection Register	0x81–0x84	Factory Protection Register Data
64-bit User-Programmable Protection Register	0x85–0x88	User Protection Register Data
Lock Register 1	0x89	Protection Register Data
128-bit User-Programmable Protection Registers	0x8A–0x109	PR-LK1

2.2 Program Protection Register

The Program Protection Register command is issued followed by the 16 bit data to be programmed. Refer to Table 1, "Read Identifier Table" on page 3. See also Figure 4, "Protection Register Programming Flowchart" on page 9. Issuing the Program Protection Register command outside of the Protection Register's address space causes a program error (SR[4] set). Attempting to program a locked Protection Register causes a program error (SR[4] set) and a lock error (SR[1] set).

2.3 Lock Protection Register

Each of the Protection Registers are lockable by programming their respective lock bits in the PR-LOCK0 or PR-LOCK1 registers as shown in Table 1. The bits in both PR-LOCK registers are also made from "OTP cells" that may be programmed to '0' but may never be erased back to '1'. The physical address of the PR-LOCK0 and PR-LOCK1 register are 0x80h and 0x89h respectively as shown in Table 1 and Figure 1, "Protection Register Map" on page 2.

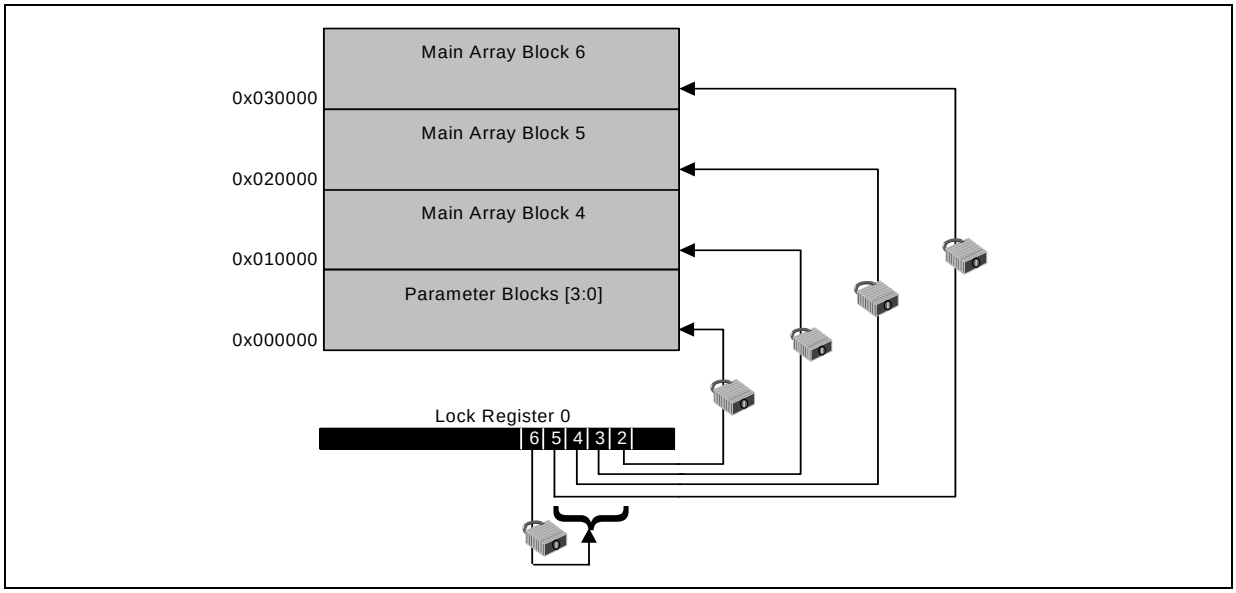
Within the PR-LOCK0, bit 0 is pre-programmed by Numonyx to lock-in a unique device number. Bit 1 of the Lock-Register -0 may be programmed by the user to lock the upper 64-bit portion (0x85h - 0x88h) once it has been programmed to the desired data pattern.

PR-LOCK1 controls the locking of the upper sixteen 128-bit Protection Registers. The PR-LOCK1 register is physically located at the address 89h as shown in Table 1 and Figure 1, "Protection Register Map" on page 2. Each of the 16 bits of the PR-LOCK1 register maps to one of the 16, 128-bit Protection Registers between 0x8A and 0x109 as shown in Table 1 and Figure 1, "Protection Register Map" on page 2. Programming a bit (to '0') in PR-LOCK1 locks the corresponding 128-bit Protection Register. After PR-LOCK register bits have been programmed, no further changes can be made to the Protection Registers' stored values. Protection commands written to a locked section result in a Status register error (Program Error bit SR-4 and Lock Error bit SR-1 are set to 1). Once locked, Protection Register states are not reversible.

3.0 "Simple" - 512 KB Protection Locking

With this option, four 128 KB sections from the Main Memory array (parameter blocks ganged together + three main blocks) may be configured as One-Time Programmable (OTP) so further program and erase operations are not allowed within the Main Memory array (see Table 2, "512K "Simple" OTP Block Mapping" on page 4). This is achieved by programming bits 2, 3, 4, and/or 5 in PR-LOCK0 at address 0x80h. Bit 6 in PR-LOCK0 is the Configuration Lock bit that prevents further programming of PR-LOCK0 bits 2, 3, 4 or 5. Once bit 6 is programmed, further programming of the OTP lock bits 2, 3, 4 or 5 is disabled. Follow the Program Protection Register command (C0h) sequence as outlined in the P30 or P33 datasheet to program these bits.

Figure 2: Selectable (Simple) OTP Locking Diagram (Bottom Boot Example)



Note: Bits 0 and 1 in Lock Register 0 function independent from the OTP Lock bits.

Table 2: 512K "Simple" OTP Block Mapping (Sheet 1 of 2)

Density	Lock Register 0 definition	Top Parameter Configuration	Bottom Parameter Configuration
256-Mbit	bit 2	blocks 258:255 (parameters)	blocks 3:0 (parameters)
	bit 3	block 254 (main)	block 4 (main)
	bit 4	block 253 (main)	block 5 (main)
	bit 5	block 252 (main)	block 6 (main)
	bit 6	Configuration Lock Bit	Configuration Lock Bit
128-Mbit	bit 2	blocks 130:127 (parameters)	blocks 3:0 (parameters)
	bit 3	block 126 (main)	block 4 (main)
	bit 4	block 125 (main)	block 5 (main)
	bit 5	block 124 (main)	block 6 (main)
	bit 6	Configuration Lock Bit	Configuration Lock Bit

Table 2: 512K "Simple" OTP Block Mapping (Sheet 2 of 2)

Density	Lock Register 0 definition	Top Parameter Configuration	Bottom Parameter Configuration
64-Mbit	bit 2	blocks 66:63 (parameters)	blocks 3:0 (parameters)
	bit 3	block 62 (main)	block 4 (main)
	bit 4	block 61 (main)	block 5 (main)
	bit 5	block 60 (main)	block 6 (main)
	bit 6	Configuration Lock Bit	Configuration Lock Bit

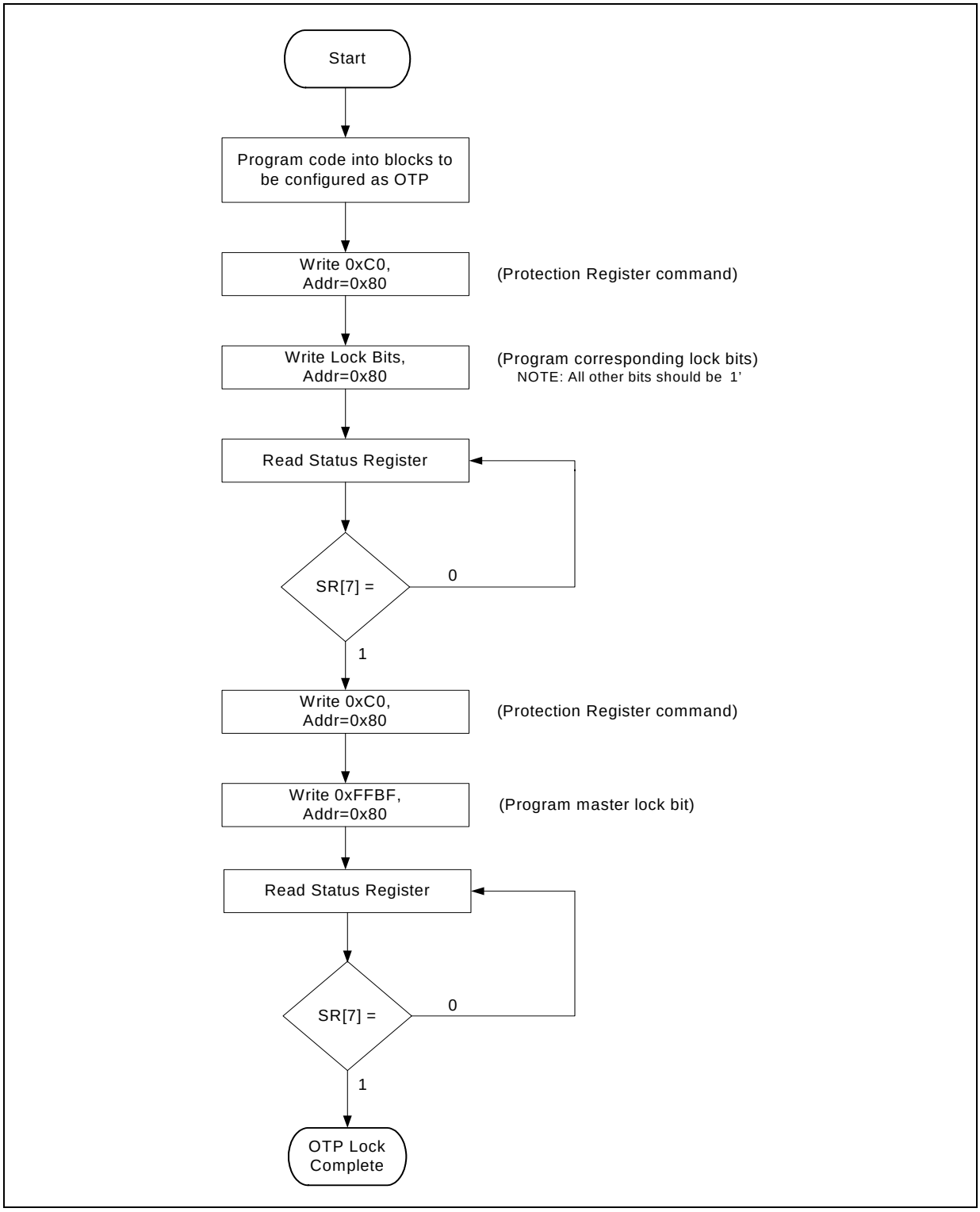
Notes:
1. When programming the OTP bits in PR-LOCK0 for a Top Parameter Device, the following upper address bits must also be driven properly: A[Max:17] driven high (V_{IH}) for TSOP and Easy BGA packages and A[Max:16] driven high (V_{IH}) for QUAD+ SCSP.
2. The 512-Mbit device will have two Selectable OTP Areas based upon two- 256-Mbit die in the stack.
3. For a complete Memory Map refer to the Numonyx™ P30 and P33 Flash Memory (65nm) Datasheet.

Read operation in these blocks is supported regardless of the state of their corresponding protection Lock bits. Program and erase operations in the main memory blocks are allowed until the block's OTP bit is programmed and when the block's flexible block locking state is unlocked (see Table 7, "Block Lock Status" on page 10).

Note: In the case of a 512M Die, following considerations need to be taken into account:

- There are 2 dice in the 512M within a virtual address space. One die is a bottom parameter die and the other die is a top parameter die.
- In order to use the block locking features on both dice, the OTP Protection Registers will need to be programmed twice, one for the bottom die and second for the top die.
- For further information on 512M device address, refer to the P30 or P33 datasheet.

Figure 3: OTP Lock Programming Flowchart



4.0 "Device" Full Array Protection Locking

This special ordered configuration allows any Main Memory block to be made into OTP. The locking granularity is 128KB (Main Block size); the top or bottom four Parameter blocks are locked jointly.

Permanent Block Locking in the Main Memory array is achieved by programming the Protection Register blocks' corresponding bit as mapped in the Protection Register space (starting at offset ECh for each density). Specific addresses within the Protection Register are used to map to the Main Memory. Programming these Protection Register bits makes the corresponding (mapped) Main Memory array into OTP. Care must be taken not to use the mapped Protection Register addresses for standard Protection Register use. Refer to Table 3 and Table 5 for details on use of the Protection Register mapping for this option.

Table 3: "Device" OTP Lock Bit Protection Register Memory Map - Bottom Boot

Table 4.

256M Bottom Boot				128M Bottom Boot		64M Bottom Boot	
OTP Address(1)	Main Memory Blocks	OTP Address(1)	Main Memory Blocks	OTP Address(1)	Main Memory Blocks	OTP Address(1)	Main Memory Blocks
109h	258: 243	F9h	130: 115	F9h	130: 115	F1h	66: 51
108h	242: 227	F8h	114: 99	F8h	114: 99	F0h	50: 35
107h	N/A(2)	F7h	N/A(2)	F7h	N/A(2)	EFh	N/A(2)
106h		F6h		F6h		EEh	
105h	226: 211	F5h	98: 83	F5h	98: 83	EDh	34: 19
104h	210: 195	F4h	82: 67	F4h	82: 67	ECh(3)	18: 0
103h	N/A(2)	F3h	N/A(2)	F3h	N/A(2)		
102h		F2h		F2h			
101h	194: 179	F1h	66: 51	F1h	66: 51		
100h	178: 163	F0h	50: 35	F0h	50: 35		
FFh	N/A(2)	EFh	N/A(2)	EFh	N/A(2)		
FEh		EEh		EEh			
FDh	162: 147	EDh	34: 19	EDh	34: 19		
FCh	146: 131	ECh(3)	18: 0	ECh(3)	18: 0		
FBh	N/A(2)						
FAh							

Notes:

1. For Bottom Boot, the *highest* numbered OTP bit locks the *highest* numbered block. For example, programming bit 15 of OTP address F1h permanently locks Block 66, and bit 0 permanently locks Block 51.
2. Available as OTP Protection Registers as described in Section 2.0, ""Standard" System Protection Registers" on page 1.
3. Programming bit 0 of the 16-bit OTP register addressed at ECh permanently locks all four Main Memory parameter blocks (Blocks 0-3). Programming bit 1of the 16-bit OTP register addressed at ECh permanently locks block 4 of the Main Memory, etc.

Table 5: OTP Lock Bit Protection Register Memory Map - Top Boot

Table 6.

256M Top Boot			
OTP Address(1)	Main Memory Blocks	OTP Address(1)	Main Memory Blocks
109h	0: 15	F9h	128: 143
108h	16: 31	F8h	144: 159
107h	N/A(2)	F7h	N/A(2)
106h		F6h	
105h	32: 47	F5h	160: 175
104h	48: 63	F4h	176: 191
103h	N/A(2)	F3h	N/A(2)
102h		F2h	
101h	64: 79	F1h	192: 207
100h	80: 95	F0h	208: 223
FFh	N/A(2)	EFh	N/A(2)
FEh		EEh	
FDh	96: 111	EDh	224: 239
FCh	112: 127	ECh(3)	240: 258
FBh	N/A(2)		
FAh			

128M Top Boot	
OTP Address(1)	Main Memory Blocks
F9h	0: 15
F8h	16: 31
F7h	N/A(2)
F6h	
F5h	32: 47
F4h	48: 63
F3h	N/A(2)
F2h	
F1h	64: 79
F0h	80: 95
EFh	N/A(2)
EEh	
EDh	96: 111
ECh(3)	112: 130

64M Top Boot	
OTP Address(1)	Main Memory Blocks
F1h	0: 15
F0h	16: 31
EFh	N/A(2)
EEh	
EDh	32: 47
ECh(3)	48: 66

Notes:

1. For Top Boot, the *highest* numbered OTP bit locks the *lowest* numbered block. For example, programming bit 15 of OTP address F1h permanently locks Block 192 on 256M, and bit 0 permanently locks Block 207.
2. Available as OTP Protection Registers as described in Section 2.0, ""Standard" System Protection Registers" on page 1.
3. Programming bit 0 of the 16-bit OTP register addressed at ECh permanently locks all four Main Memory parameter blocks (Blocks 255:258). Programming bit 1of the 16-bit OTP register addressed at ECh permanently locks block 254 of the Main Memory, etc.
4. For Top Boot Only: when programming the OTP bits in PR-LR0, the following upper address bits must also be driven properly: A[Max:17] driven high[Vih] for TSOP and EZBGA packages and A[Max:16] driven high[Vih] for Quad + SCSP packages.

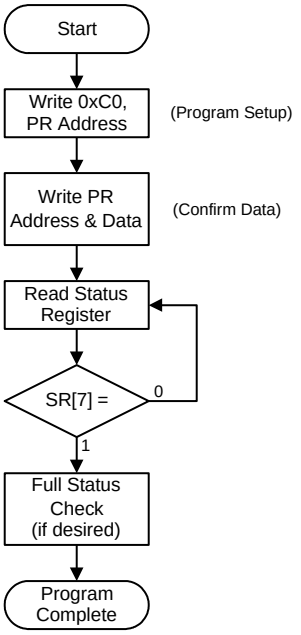
PR-LOCK1 (offset 89h in ID Memory Space) contains the master lock bits for the 2K OTP space. Further details are described in Section 2.0, ""Standard" System Protection Registers" on page 1. Programming the 2K OTP address space or the PR-LOCK1 register is not allowed during Erase Suspends. WP# has no effect on the lock bits or the blocks that are permanently locked.

Note: In the case of a 512M Die, following considerations need to be taken into account:

- There are 2 dice in the 512M within a virtual address space. One die is a bottom parameter die and the other die is a top parameter die.
- In order to use the block locking features on both dice, the OTP Protection Registers will need to be programmed twice, one for the bottom die and second for the top die.
- For further information on 512M device address, refer to the P30 or P33 datasheet.

Figure 4: Protection Register Programming Flowchart

PROTECTION REGISTER PROGRAMMING PROCEDURE



Bus Operation	Command	Comments
Write	Program PR Setup	Data = 0xC0 Addr = First Location to Program
Write	Protection Program	Data = Data to Program Addr = Location to Program
Read	None	Status Register Data.
Idle	None	Check SR[7]: 1 = WSM Ready 0 = WSM Busy

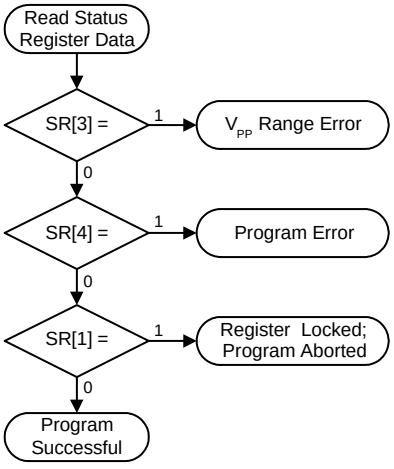
Program Protection Register operation addresses must be within the Protection Register address space. Addresses outside this space will return an error.

Repeat for subsequent programming operations.

Full Status Register check can be done after each program, or after a sequence of program operations.

Write 0xFF after the last operation to set Read Array state.

FULL STATUS CHECK PROCEDURE



Bus Operation	Command	Comments
Idle	None	Check SR[3]: 1 =V_{PP} Range Error
Idle	None	Check SR[4]: 1 =Programming Error
Idle	None	Check SR[1]: 1 =Block locked; operation aborted

Only the Clear Staus Register command clears SR[1, 3, 4].

If an error is detected, clear the Status register before attempting a program retry or other error recovery.

Caution: **Once blocks are locked using the OTP Protection Registers, it will override the normal Flexible block locking of main array blocks. Issuing a program or erase command on an OTP locked block will result in a failure regardless of the flexible block locking status. The Status Register will set SR[4,1] for a program failure or SR[5,1] for an erase failure. Refer to** Table 7, "Block Lock Status"**.**

Table 7: Block Lock Status

Flexible Block Locking Status	OTP Block Locking Status	Actual Block Status
Unlocked	Unlocked	Unlocked
Locked	Unlocked	Locked
Lock-Down	Unlocked	Lock-Down
X	Locked	Locked

5.0 Ordering Information

Table 8: P30 Ordering Information

P30 Part Number	S-Spec	Special Feature	MM#	Media
PC28F256P30B85	S L9C4	Device OTP	880699	T/R
PC28F256P30B85	S LA9E	Device OTP	890210	Tray
PC28F256P30B85	S L8X7	Simple OTP	876079	T/R
PC28F128P30B85	S L9M6	Device OTP	883232	T/R
PC28F128P30B85	S L9YQ	Device OTP	887046	Tray
PC28F128P30B85	S L8WY	Simple OTP	876069	T/R
PC28F640P30B85	S L9M2	Device OTP	883222	T/R
PC28F640P30B85	S LA9D	Device OTP	890209	Tray
PC28F640P30B85	S L8XB	Simple OTP	876094	T/R

Table 9: P33 Ordering Information

P33 Part Number	S-Spec	Special Feature	MM#	Media
PC48F4400P0TB00	S LAFB	Device OTP	891111	Tray
PC48F4400P0TB00	S LAFC	Device OTP	891112	T/R
PC28F256P33B85	S L9R6	Device OTP	884123	T/R
PC28F256P33B85	S LA8F	Device OTP	889994	Tray
PC28F128P33B85	S LA37	Device OTP	888020	Tray
PC28F128P33B85	S LA4N	Device OTP	888347	T/R
PC28F640P33B85	S LA8S	Device OTP	890075	T/R
PC28F640P33B85	S LA8T	Device OTP	890076	Tray
PC28F640P33T85	S LAAM	Simple OTP	890394	T/R

Note: Additional line items available by request. Please contact your Numonyx Sales Representative for more information.

Figure 5: Decoder for Descrete Products

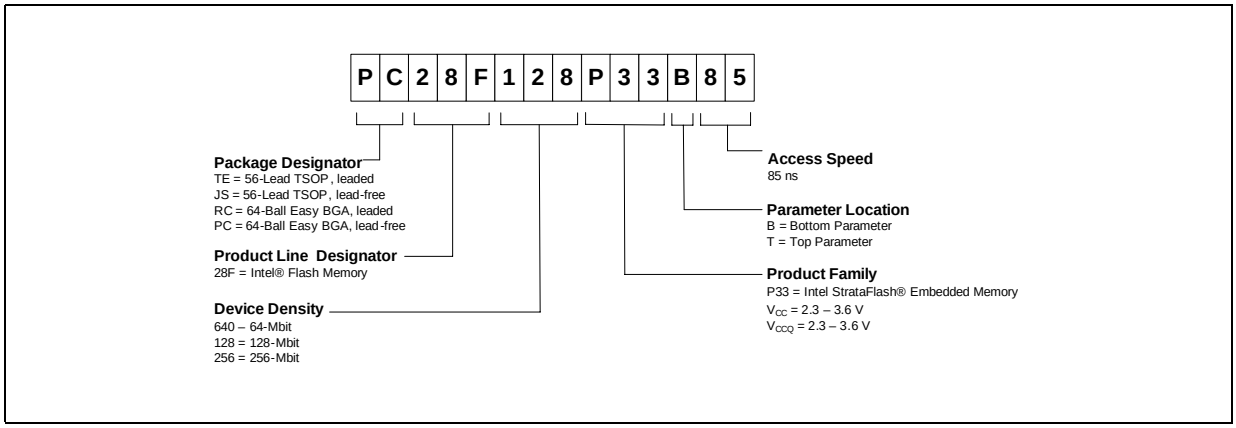
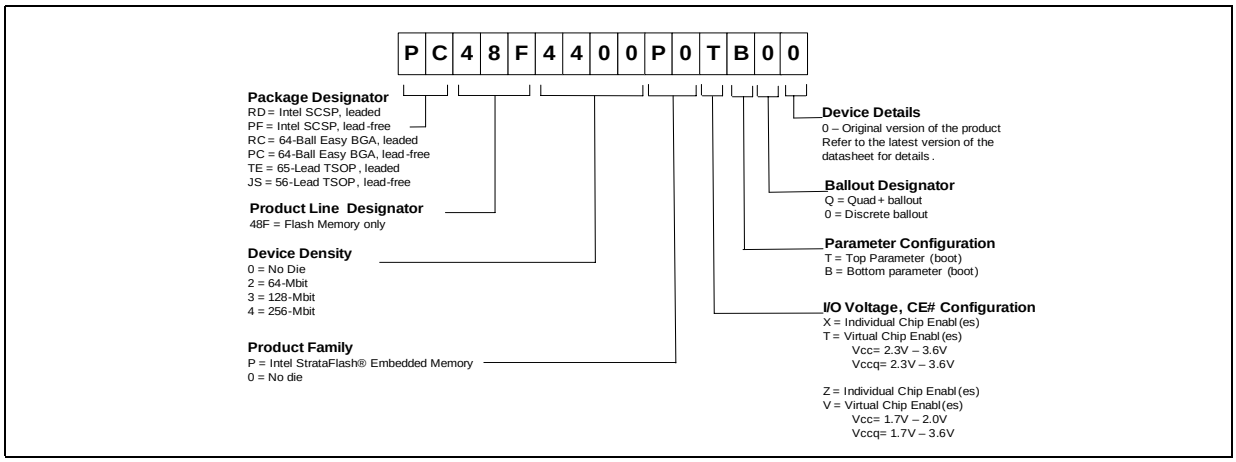


Figure 6: Decoder for SCSP Products



Note: For differentiation purposes on all packages, Simple OTP parts will have a "B" marked after the <FPO> and Full Device OTP parts will have a "D" marked after the <FPO>.