How to Use OTP Registers for Security Applications

Application Note 717

October 1999

Order Number: 292265-001

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature may be obtained by calling 1-800-548-4725 or by visiting Intel's website at http://www.intel.com.

Contents

Revision History

Date of Revision	Version	Description
10/13/99	-001	Original version

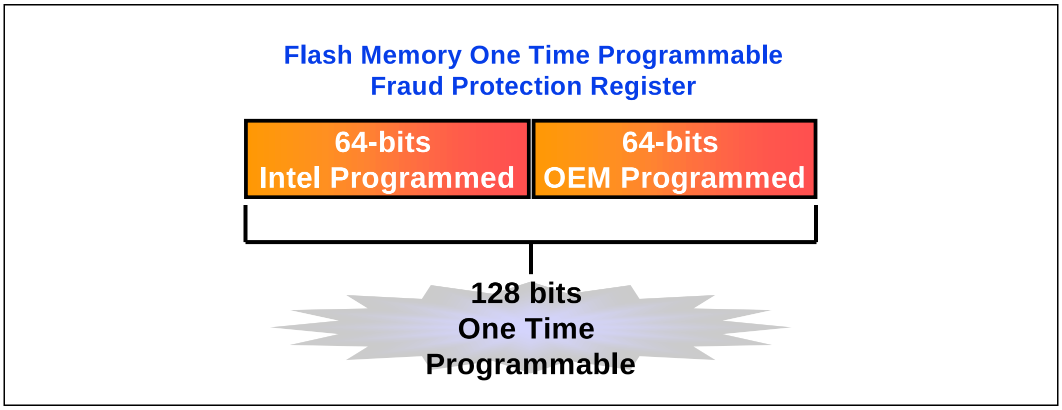
1.0 Introduction

The 3 Volt Intel® StrataFlash™ memory includes a 128-bit protection register that can be used to increase the security of a system design by allowing tracking and fraud protection. For example, the number contained in the protection register can be used to match the flash component with other system components such as the CPU or ASIC, preventing device substitution.

2.0 What Is OTP?

OTP means "One Time Programmable." The 3 Volt Intel StrataFlash components include a 128-bit OTP register. The 128-bits of the protection register are divided into two 64-bit segments. One of the segments is programmed at the Intel factory with a unique 64-bit number, which cannot be changed. The other segment is left blank for customer designers to program as desired. For a graphical illustration see Figure 1. Once the customer segment is programmed, it can be locked to prevent reprogramming. This lock cannot be reversed by the customer.

Figure 1. Flash OTP Fraud Protection Register



3.0 Using the Protection Register

The following sections describe the operation for reading and programming the Protection Register.

3.1 Reading the Protection Register

The protection register is read in the identification read mode. The flash device is switched to this mode by writing the Read Identifier command (90H). Once in this mode, read cycles from addresses shown in Table 1 or Table 2 retrieve the protection register information. To return to read array mode, write the Read Array command (FFH).

Table 1. Word-Wide Protection Register Addressing

Word	Use	ID Offset	A8	A7	A6	A5	A4	A3	A2	A1
LOCK	Both	0080h	1	0	0	0	0	0	0	0
0	Intel	0080h	1	0	0	0	0	0	0	1
1	Intel	0082h	1	0	0	0	0	0	1	0
2	Intel	0083h	1	0	0	0	0	0	1	1
3	Intel	0084h	1	0	0	0	0	1	0	0
4	Customer	0085h	1	0	0	0	0	1	0	1
5	Customer	0086h	1	0	0	0	0	1	1	0
6	Customer	0087h	1	0	0	0	0	1	1	1
7	Customer	0088h	1	0	0	0	1	0	0	0

NOTE: 1. All address lines not specified in the above table must be 0 when accessing the Protection Register, i.e., A_{23}–A_9 = 0.

Table 2. Byte-Wide Protection Register Addressing

Byte	Use	ID Offset	A8	A7	A6	A5	A4	A3	A2	A1
LOCK	Both	80h	1	0	0	0	0	0	0	0
LOCK	Both	80h	1	0	0	0	0	0	0	0
0	Customer	81h	1	0	0	0	0	0	0	1
1	Customer	81h	1	0	0	0	0	0	0	1
2	Customer	82h	1	0	0	0	0	0	1	0
3	Customer	82h	1	0	0	0	0	0	1	0
4	Customer	83h	1	0	0	0	0	0	1	1
5	Customer	83h	1	0	0	0	0	0	1	1
6	Customer	84h	1	0	0	0	0	1	0	0
7	Customer	84h	1	0	0	0	0	1	0	0
8	Intel	85h	1	0	0	0	0	1	0	1
9	Intel	85h	1	0	0	0	0	1	0	1
A	Intel	86h	1	0	0	0	0	1	1	0
B	Intel	86h	1	0	0	0	0	1	1	0
C	Intel	87h	1	0	0	0	0	1	1	1
D	Intel	87h	1	0	0	0	0	1	1	1
E	Intel	88h	1	0	0	0	1	0	0	0
F	Intel	88h	1	0	0	0	1	0	0	0

NOTE: 1. All address lines not specified in the above table must be 0 when accessing the Protection Register, i.e., A_{23}–A_9 = 0.

3.2 Programming the Protection Register

The protection register bits are programmed using the two-cycle Protection Program command shown in Figure 3. The 64-bit number is programmed 16 bits at a time for x16 mode. First write the Protection Program Setup command, C0H. The next write to the device will latch in the address and data, and program the specified location. The allowable addresses are shown in Table 1 or Table 2. See Figure 2, “Protection Register Programming Flowchart” on page 4.

Any attempt to address Protection Program commands outside the defined protection register address space will result in a status register error (program error bit SR.4 will be set to 1). See Table 4 for Status Register Definitions. Attempting to program a locked protection register segment will result in a status register error (program error bit SR.4 and lock error bit SR.1 will be set to 1).

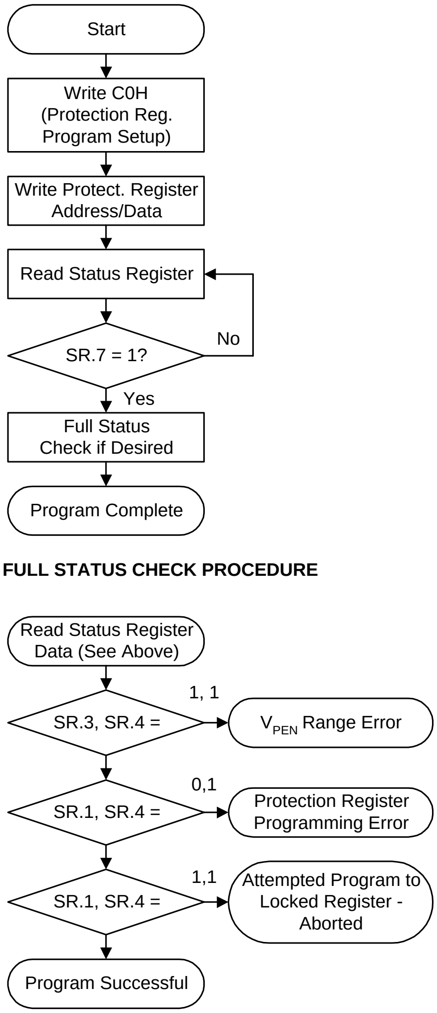
Table 3. Intel® StrataFlash™ Memory Command Set Definitions(1)

Command	Bus Cycles Req’d.	First Bus Cycle			Second Bus Cycle		
		Oper	Addr(2)	Data(3,4)	Oper	Addr(2)	Data(3,4)
Protection Program	2	Write	X	C0H	Write	PA	PD

NOTES:

1. Commands other than those shown above are reserved by Intel for future device implementations and should not be used.
2. X = Any valid address within the device.
   PA = Address of memory location to be programmed.
   ID = Data read from Identifier Codes.
3. PD = Data to be programmed at location PA. Data is latched on the rising edge of WE#.
4. The upper byte of the data bus (DQ_8–DQ_{15}) during command writes is a “Don’t Care” in x16 operation.

Figure 2. Protection Register Programming Flowchart



Bus Operation	Command	Comments
Write	Protection Program Setup	Data = C0H

Write	Protection Program	Data = Data to Program
		Addr = Location to Program

Read		Status Register Data Toggle CE# or OE# to Update Status Register Data
Standby		Check SR.7 1 = WSM Ready 0 = WSM Busy

Protection Program operations can only be addressed within the protection register address space. Addresses outside the defined space will return an error.

Repeat for subsequent programming operations.

SR Full Status Check can be done after each program or after a sequence of program operations.

Write FFH after the last program operation to reset device to read array mode.

Bus Operation	Command	Comments
Standby		SR.1 SR.3 SR.4 0 1 1 V_{PEN} Low
Standby		0 0 1 Prot. Reg. Prog. Error
Standby		1 0 1 Register Locked: Aborted

SR.3 MUST be cleared, if set during a program attempt, before further attempts are allowed by the Write State Machine.

SR.1, SR.3 and SR.4 are only cleared by the Clear Staus Register Command, in cases of multiple protection register program operations before full status is checked.

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

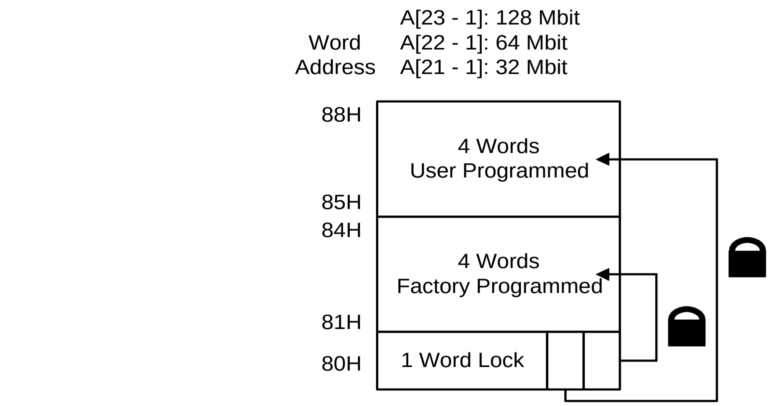
Table 4. Status Register Definitions

<table>
<tr><th>WSMS</th><th>ESS</th><th>ECLBS</th><th>PSLBS</th><th>VPENS</th><th>R</th><th>DPS</th><th>R</th></tr>
<tr><td>bit 7</td><td>bit 6</td><td>bit 5</td><td>bit 4</td><td>bit 3</td><td>bit2</td><td>bit 1</td><td>bit 0</td></tr>
<tr><td>High Z When Busy?</td><td colspan="4">Status Register Bits</td><td colspan="3">Notes</td></tr>
<tr><td>No</td><td colspan="4">SR.7 = WRITE STATE MACHINE STATUS
1 = Ready
0 = Busy</td><td colspan="3" rowspan="8">Check STS or SR.7 to determine block erase, program, or lock-bit configuration completion. SR.6–SR.0 are not driven while SR.7 = “0.”
If both SR.5 and SR.4 are “1”s after a block erase or lock-bit configuration attempt, an improper command sequence was entered.
SR.3 does not provide a continuous programming voltage level indication. The WSM interrogates and indicates the programming voltage level only after Block Erase, Program, Set Block Lock-Bit, or Clear Block Lock-Bits command sequences.
SR.1 does not provide a continuous indication of block lock-bit values. The WSM interrogates the block lock-bits only after Block Erase, Program, or Lock-Bit configuration command sequences. It informs the system, depending on the attempted operation, if the block lock-bit is set. Read the block lock configuration codes using the Read Identifier Codes command to determine block lock-bit status.
SR.0 is reserved for future use and should be masked when polling the status register.</td></tr>
<tr><td>Yes</td><td colspan="4">SR.6 = ERASE SUSPEND STATUS
1 = Block Erase Suspended
0 = Block Erase in Progress/Completed</td></tr>
<tr><td>Yes</td><td colspan="4">SR.5 = ERASE AND CLEAR LOCK-BITS STATUS
1 = Error in Block Erasure or Clear Lock-Bits
0 = Successful Block Erase or Clear Lock-Bits</td></tr>
<tr><td>Yes</td><td colspan="4">SR.4 = PROGRAM AND SET LOCK-BIT STATUS
1 = Error in Setting Lock-Bit
0 = Successful Set Block Lock Bit</td></tr>
<tr><td>Yes</td><td colspan="4">SR.3 = PROGRAMMING VOLTAGE STATUS
1 = Low Programming Voltage Detected, Operation Aborted
0 = Programming Voltage OK</td></tr>
<tr><td>Yes</td><td colspan="4">SR.2 = PROGRAM SUSPEND STATUS
1 = Program suspended
0 = Program in progress/completed</td></tr>
<tr><td>Yes</td><td colspan="4">SR.1 = DEVICE PROTECT STATUS
1 = Block Lock-Bit Detected, Operation Abort
0 = Unlock</td></tr>
<tr><td>Yes</td><td colspan="4">SR.0 = RESERVED FOR FUTURE ENHANCEMENTS</td></tr>
</table>

3.3 Locking the Protection Register

The user-programmable segment of the protection register is lockable by programming Bit 1 of the PR-LOCK location to 0. The *Protection Register Memory Map* is shown in Figure 3 on page 6. Bit 0 of this location is programmed to 0 at the Intel factory to protect the unique device number. Bit 1 is set using the Protection Program command to program “FFFD” to the PR-LOCK location. After these bits have been programmed, no further changes can be made to the values stored in the protection register. Protection Program commands to a locked section will result in a status register error (program error bit SR.4 and Lock Error bit SR.1 will be set to 1). Protection register lockout state is not reversible.

Figure 3. Protection Register Memory Map



4.0 Additional Information

Order Number	Document/Tool
290667	*3 Volt Intel® StrataFlash™ Memory; 28F128J3A, 28F640J3A, 28F320J3A* datasheet

NOTE:
1. Please call the Intel Literature Center at (800) 548-4725 to request Intel documentation. International customers should contact their local Intel or distribution sales office.
2. Visit Intel’s World Wide Web home page at http://www.intel.com for technical documentation and tools