



General Description

This supplementary document provides information on secure model devices, designed for limited distribution. It describes how the features, operation, and ordering options of these devices have been enhanced or changed from the standard devices on which they are based. The information contained in this document modifies any information on the same topics established by the datasheets listed in the [Affected Documents/Related Documents](#) table and should be used in conjunction with those documents. This document may also contain information that was not previously covered by the S25FL512S/S70FL01GS datasheet. It is intended for hardware system designers and software developers of applications, operating systems, or tools.

Affected Documents/Related Documents

Title	Publication Number
S25FL512S Datasheet	001-98284
S70FL01GS Datasheet	001-98295

1. Device Description

1.1 Permanent Lock Description

The device offers a unique Permanent Lock feature that allows the host system to permanently secure data in the memory array. Initiating this locking feature makes the selected block protection scheme permanent, thereby disabling both program and erase operations in the protected region of the array.

1.2 Advanced Sector Protection Description

The secure model devices modify the Advanced Sector Protection (ASP) features:

- All Dynamic Protection Bits (DYB) are modified to be in the protected state following power-up
- All Persistent Protection Bits (PPB) are modified to be One Time Programmable (OTP). After a PPB bit is programmed, the related sector is permanently protected. PPB bits are not erasable. PPB bits may be programmed while the PPBLOCK Bit = 0.

2. Registers

2.1 Configuration Register 1 (CR1)

Bit 4 called LOCK is added to CR1. When set to 1, the Block Protection configuration is permanent.

Table 1. Configuration Register (CR1)

Bits	Field Name	Function	Default State	Description
7	LC1	Latency Code	0	Selects number of initial read latency cycles. See Latency Code Tables
6	LC0		0	
5	TBPROT	Configures Start of Block Protection and selects readable boot sector in Read Password Mode	0	1 = BP starts at bottom (Low address) 0 = BP starts at top (High address)
4	LOCK	Permanently locks BP2-0 and TBPROT bits in their state when LOCK is set to 1	0	1 = Locked 0 = Un-locked
3	BPV	Configures BP2-0 in Status Register	0	1 = Volatile 0 = Non-Volatile
2	RFU	RFU	RFU	Reserved for Future Use
1	QUAD	Puts the device into Quad I/O operation	0	1 = Quad 0 = Dual or Serial
0	FREEZE	Lock current state of BP2-0 bits in Status Register and TBPROT in Configuration Register, and OTP regions	0	1 = Block Protection and OTP locked 0 = Block Protection and OTP un-locked

2.2 ASP Register (ASPR)

Bits 3 and 4 are added to make PPB bits OTP and DYB bits default to protected state following power-up.

Table 2. ASP Register (ASPR)

Bits	Field Name	Function	Default State	Description
15 to 9	RFU	Reserved	1	Reserved for Future Use
8	RFU	Reserved	0	Reserved for Future Use
7	RFU	Reserved	0	Reserved for Future Use
6	RFU	Reserved	1	Reserved for Future Use
5	RFU	Reserved	1	Reserved for Future Use
4	DYBLBB	DYB Lock Boot Bit	0	0 = All DYB power-up in the protected state (0)
3	PPBOTP	PPB OTP Bit	0	0 = PPB bits are OTP
2	PWDMLB	Password Protection Mode Lock Bit	1	0 = Password Protection Mode permanently enabled. 1 = Password Protection Mode not permanently enabled.
1	PSTMLB	Persistent Protection Mode Lock Bit	1	0 = Persistent Protection Mode permanently enabled. 1 = Persistent Protection Mode not permanently enabled.
0	RFU	Reserved	1	Reserved for Future Use

3. Block Protection

3.1 Lock Bit

Bit 4 of the Configuration Register is the LOCK bit. When the LOCK bit is programmed to a 1 the BP2-0 bits in the Status Register and the TBPROT bit in the Configuration Register are permanently locked to their nonvolatile values, they cannot be erased or programmed; thereby permanently locking the selected portion of the memory array from change by programming or erasure. The FREEZE bit and BPNV bits in the Configuration Register no longer affect the BP2-0 bits, because the LOCK bit has permanently frozen the BP2-0 bits in their non-volatile state. Any attempt to change the BP bits with the WRR command while LOCK = 1 is ignored and no error status is set. The LOCK bit is a one-time programmable value, so once set it cannot be changed back.

4. Advanced Sector Protection

4.1 ASP Register

The ASP register is used to permanently configure the behavior of Advanced Sector Protection (ASP) features.

The ASPR[4] DYB Lock Boot Bit is shipped from the factory as 0, which means all the DYB are powered up in the Protected State.

The ASPR[3] PPB OTP Bit is shipped from the factory as 0, which means all the PPB bits are One Time Programmable. Once a PPB bit is programmed to 0, the related sector is permanently protected.

The PPBLOCK bit controls when PPB bits are programmable or protected as described in the standard device models data sheet. The Persistent and Password protection modes control the PPBLOCK bit state as described in the standard device models data sheet.

4.2 Read Password Protection Mode

If enabled the Read Password Method is a security option that will replace the default PPB Password Protection Mode. The Read Password Protection Mode enables protecting the main Flash array from read, program and erase. Only the lowest or highest address range, selected by the configuration register TBPROT bit, remains readable until a successful Password Unlock command is completed.

In this mode the PPB Lock bit is used to control the high order bits of address. When the PPB Lock bit is 1, the address bits operate normally. When the PPB Lock bit is 0, the address bits that select a main array sector address range are forced either to Zeros (TBPROT = 0) or to Ones (TBPROT = 1) to select the lowest or highest address main Flash array address range per the table below. When TBPROT is cleared to a 0, the bottom (zero address) 64 KB or 256 KB of the array is readable. When TBPROT is set to a 1, the top (maximum address) 64 KB or 256 KB of the array is readable. The selection of 64 KB or 256 KB depends on the OPN selection for size of the sector erase command.

Sector size option	TBPARAM = 0 (bottom of the chip)		TBPARAM = 1 (top of the chip)	
	TBPROT = 0	TBPROT = 1	TBPROT = 0	TBPROT = 1
64 KB (Hybrid)	User is confined to the lowest address sixteen 4 KB sectors.	User is confined to the highest address 64 KB sector	User is confined to the lowest address 64 KB sector	User is confined to the highest address sixteen 4 KB sectors
256 KB (Uniform) TBPARAM is ignored	User is confined to the lowest address sector	User is confined to highest address sector	User is confined to the lowest address sector	User is confined to highest address sector

This address range selection is independent of the bank address register. The Bank Address Register remains at the default value of zero. The BRWR command does not work during read password mode so the user must be aware to set the BAR to the desired address immediately after the password unlock to normal read mode.

The PPB bits are protected from program and erase when PPB Lock is 0 and may be programmed or erased when PPB Lock is 1.

The PPB Lock bit is set to 0 by power-on reset or hardware reset — same as in PPB Password Protection Mode.

Read Password Protection Notes:

1. The user can program the ASPR[5] bit to 0 and use read password, or not, as desired.
2. The command sequence for programming, reading, and locking of the Password for Read Password Method is the same as the default for the PPB Password Method.

3. When the Read Password Mode and Password Protection Mode are enabled (i.e. ASPR[2] and ASPR[5] are programmed to 0), then all addresses are redirected to the Boot Sector until the password unlocking sequence is properly entered, with the correct password. At which time, the Read Password Mode is disabled and all addressing will select the proper location.
4. If a system hardware reset occurs, then the Read Password Mode is re-enabled.
5. ASPR[5] is used to select between Read Password vs. PPB Password options. If ASPR[5]=0 then the device is ready for Read Password. However, Read Password is not enabled until ASPR[2]=0. At which point, all addresses select only within the top or bottom sectors, until the device is unlocked with the proper unlocking sequence and Password. When ASPR[2] is not = 1 the addresses select normally. This allows users to program in code, test it, provide a password, and then lock it by programming ASPR[2]= 0.
6. The PLBWR command has undefined results if sent when Read Password Protection is in use. The PPB Lock bit may only be returned to 0 by a hardware reset or power-on reset.
7. Only the read commands and the Password Unlock command are valid during Read Password Mode while the PPB Lock bit = 1. Other commands are disabled until the password is supplied to enable reading of the entire device and normal command operation.
8. When Read Password Protection mode is active (ASPR[5]=0, ASPR[2]=0, PPB Lock = 0), reading of the main array is allowed but forced to have only the boot sector visible via the forcing of memory sector address to zero or ones. Reading the OTP, DYB, and PPB address space returns undefined data.
9. Programming memory spaces or writing registers is not allowed when Read Password Protection mode is active. The WRR, WRDI, WREN, ABWR, BRWR, ASPP, CLSR, OTPP, PNVDLR, WVDLR, PLBWR, DYBWR, PPBP, PPBE and PASSP commands do not change memory or register state when Read Password Protection mode is active. RESET operates normally, and bus protocol may be modified by resetting mode bits.
10. AutoBoot is disabled when the Read Password feature is enabled, as part of the ASP. This removes any conflicts when the AutoBoot address is within the Protected Area. The user won't be able to AutoBoot since a password is required prior to addressing the "boot" code. Cypress recommends that the ABE Bit 0 should be cleared to 0 when the Read Password feature is enabled.
11. All ID Read commands - ABh, 90h, 9Fh, and 5Ah (FL512S only) - are enabled and can be used when the device is in Read Password Protection mode.
12. The BRAC and WRR combined command sequence is illegal when Read Password mode is active, prior to the password being provided.

5. Commands

5.1 Reset Commands

5.1.1 Software Reset Command (RESET F0h)

The Software Reset command (RESET) restores the device to its initial power up state, except for the volatile FREEZE bit in the Configuration register CR1[1] and the volatile PPB Lock bit in the PPB Lock Register. The Freeze bit and the PPB Lock bit will remain set at their last value prior to the software reset. To clear the FREEZE bit and set the PPB Lock bit to its protection mode selected power on state, a full power-on reset sequence or hardware reset must be done. Note that all bits in the configuration register retain their previous state after a Software Reset. The Block Protection bits BP2, BP1, and BP0, in the status register will only be reset if they are configured as volatile via the BPNV bit in the Configuration Register (CR1[3]) and FREEZE (CR1[0]) is cleared to zero and LOCK (CR1[4]) is cleared to zero. The software reset cannot be used to circumvent the FREEZE or PPBLOCK bit protection mechanisms for security configuration bits (SR1[4:2], CR1[5:2], and PPB bits). The reset command is executed when CS# is brought to high state and requires t_{RPH} time to execute.

In case of power-up failure, if the user applies a RESET command, a full power up sequence is triggered. Meanwhile program and erase commands are ignored.

6. Software Interface Reference

6.1 Device ID and Common Flash Interface (ID-CFI) Address Map

CFI Alternate Vendor-Specific Extended Query Parameter 88h Data Protection

Parameter Relative Byte Address Offset	Data	Description
00h	88h	Parameter ID (Data Protection)
01h	04h	Parameter Length (The number of following bytes in this parameter. Adding this value to the current location value +1 = the first byte of the next parameter)
02h	0Ah	OTP size 2 ^N bytes, FFh = not supported
03h	01h	OTP address map format, 01h = FL-S format, FFh = not supported
04h	02h	Block Protect Type, model dependent 00h = FL-P, FL-S, FFh = not supported, 02h = FL-S Lock Bit Enabled
05h	03h	Advanced Sector Protection type, model dependent 01h = FL-S ASP, 03h = FL-S ASP with DYB Lock Boot and PPBOTP

6.2 Initial Delivery State

The ASP Register contents depend on the ordering options selected.

Table 3. Ordering Options

Ordering Part Number Model	ASPR Default Value
K1, L1, S1, T1, Y1, Z1 M1, N1, U1, V1, W1, X1	FE67h

7. Ordering Information – S25FL512S/S70FL01GS Enhanced Security

Enhanced Security devices enable an option to use a password to control read access and an option to permanently lock the Block Protection controls. The ordering part number is formed by a valid combination of the following:

S25FL	512	S	AG	B	H	I	K1	0	
									Packing Type
									0 = Tray
									1 = Tube
									3 = 13" Tape and Reel
									Model Number (Additional Ordering Options)
									P1 = Security, EHPLC, SO footprint with RESET#, uniform 256 KB sectors
									K1 = Security, EHPLC, 5x5 ball BGA footprint with RESET# and V _{IO} , uniform 256 KB sectors
									L1 = Security, EHPLC, 4x6 ball BGA footprint with RESET# and V _{IO} , uniform 256 KB sectors
									S1 = Security, EHPLC, 5x5 ball BGA footprint with RESET#, uniform 256 KB sectors
									T1 = Security, EHPLC, 4x6 ball BGA footprint with RESET#, uniform 256 KB sectors
									Y1 = Security, EHPLC, 5x5 ball BGA footprint, uniform 256 KB sectors
									Z1 = Security, EHPLC, 4x6 ball BGA footprint, uniform 256 KB sectors
									M1 = Security, HPLC, 5x5 ball BGA footprint with RESET# and V _{IO} , uniform 256 KB sectors
									N1 = Security, HPLC, 4x6 ball BGA footprint with RESET# and V _{IO} , uniform 256 KB sectors
									U1 = Security, HPLC, 5x5 ball BGA footprint with RESET#, uniform 256 KB sectors
									V1 = Security, HPLC, 4x6 ball BGA footprint with RESET#, uniform 256 KB sectors
									W1 = Security, HPLC, 5x5 ball BGA footprint, uniform 256 KB sectors
									X1 = Security, HPLC, 4x6 ball BGA footprint, uniform 256 KB sectors
									Temperature Range
									I = Industrial (–40°C to + 85°C)
									Package Materials
									H = Low-Halogen, Lead (Pb)-free
									F = Lead (Pb)-free
									Package Type
									B = 24-ball BGA 6 x 8 mm package, 1.00 mm pitch
									M = 16-pin SO package
									Speed
									AG = 133 MHz SDR
									Device Technology
									S = 65-nm MirrorBit Process Technology
									Density
									512 = 512 Mbit
									01G = 1024 Mbit
									Device Family
									S25FL
									Cypress Memory 3.0 Volt-Only, Serial Peripheral Interface (SPI) Flash Memory
									S70FL
									Cypress Stacked Memory 3.0V-Only, Serial Peripheral Interface (SPI) Flash Memory

Notes:

1. EHPLC = Enhanced High Performance Latency Code table.
2. HPLC = High Performance Latency Code table.
3. Uniform 256 KB sectors = All sectors are uniform 256 KB with a 512B programming buffer.

Valid Combinations

Valid Combinations list configurations planned to be supported in volume for this device. Contact your local sales office to confirm availability of specific valid combinations and to check on newly released combinations.

S25FL512S/S70FL01GS Valid Combinations Secure					
Base Ordering Part Number	Speed Option	Package and Temperature	Model Number	Packing Type	Package Marking
S25FL512S	AG	BHI	K1, L1, S1, T1, Y1, Z1	0, 3	FL512SAIH + (Model Number)
		MFI	P1	0, 1, 3	FL512SAIFP1
S70FL01GS	AG	MFI	P1	0, 1, 3	FL01GSAIFP1

Note:

1. Contact factory for availability.

8. Revision History

Document History Page

Document Title: S25FL512S/S70FL01GS, 512 Mbit (64 Mbyte)/1024 Mbit (128 Mbyte), 3 V MirrorBit® Flash Document Number: 002-00780				
Rev.	ECN No.	Orig. of Change	Submission Date	Description of Change
**	—	ANSI	05/09/2012	Initial release
*A	4978763	ANSI	10/21/2015	Updated to Cypress template.
*B	5532910	ECAO	01/30/2017	Updated Sales and Copyright information. Included S70FL01GS Secure Model. Updated Ordering Information – S25FL512S/S70FL01GS Enhanced Security : Added Tube Packing type. Added P1) = Security, EHPLC, SO footprint with RESET#, uniform 256 KB sectors Model Number. Added F) = Lead (Pb) - free Package Material. Added M) = 16 pin SO Package. Removed DP = 66 MHz DDR Speed option. Updated Valid Combinations Table to include S70FL01GS Secure parts.
*C	5767590	ECAO	06/09/2017	Added Section 4.2, Read Password Protection Mode on page 3 Updated logo and copyright

Sales, Solutions, and Legal Information

Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at [Cypress Locations](#).

Products

ARM® Cortex® Microcontrollers	cypress.com/arm
Automotive	cypress.com/automotive
Clocks & Buffers	cypress.com/clocks
Interface	cypress.com/interface
Internet of Things	cypress.com/iot
Memory	cypress.com/memory
Microcontrollers	cypress.com/mcu
PSoC	cypress.com/psoc
Power Management ICs	cypress.com/pmic
Touch Sensing	cypress.com/touch
USB Controllers	cypress.com/usb
Wireless Connectivity	cypress.com/wireless

PSoC® Solutions

[PSoC 1](#) | [PSoC 3](#) | [PSoC 4](#) | [PSoC 5LP](#) | [PSoC 6](#)

Cypress Developer Community

[Forums](#) | [WICED IOT Forums](#) | [Projects](#) | [Video](#) | [Blogs](#) | [Training](#) | [Components](#)

Technical Support

cypress.com/support

© Cypress Semiconductor Corporation, 2012-2017. This document is the property of Cypress Semiconductor Corporation and its subsidiaries, including Spansion LLC ("Cypress"). This document, including any software or firmware included or referenced in this document ("Software"), is owned by Cypress under the intellectual property laws and treaties of the United States and other countries worldwide. Cypress reserves all rights under such laws and treaties and does not, except as specifically stated in this paragraph, grant any license under its patents, copyrights, trademarks, or other intellectual property rights. If the Software is not accompanied by a license agreement and you do not otherwise have a written agreement with Cypress governing the use of the Software, then Cypress hereby grants you a personal, non-exclusive, nontransferable license (without the right to sublicense) (1) under its copyright rights in the Software (a) for Software provided in source code form, to modify and reproduce the Software solely for use with Cypress hardware products, only internally within your organization, and (b) to distribute the Software in binary code form externally to end users (either directly or indirectly through resellers and distributors), solely for use on Cypress hardware product units, and (2) under those claims of Cypress's patents that are infringed by the Software (as provided by Cypress, unmodified) to make, use, distribute, and import the Software solely for use with Cypress hardware products. Any other use, reproduction, modification, translation, or compilation of the Software is prohibited.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CYPRESS MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS DOCUMENT OR ANY SOFTWARE OR ACCOMPANYING HARDWARE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. To the extent permitted by applicable law, Cypress reserves the right to make changes to this document without further notice. Cypress does not assume any liability arising out of the application or use of any product or circuit described in this document. Any information provided in this document, including any sample design information or programming code, is provided only for reference purposes. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. Cypress products are not designed, intended, or authorized for use as critical components in systems designed or intended for the operation of weapons, weapons systems, nuclear installations, life-support devices or systems, other medical devices or systems (including resuscitation equipment and surgical implants), pollution control or hazardous substances management, or other uses where the failure of the device or system could cause personal injury, death, or property damage ("Unintended Uses"). A critical component is any component of a device or system whose failure to perform can be reasonably expected to cause the failure of the device or system, or to affect its safety or effectiveness. Cypress is not liable, in whole or in part, and you shall and hereby do release Cypress from any claim, damage, or other liability arising from or related to all Unintended Uses of Cypress products. You shall indemnify and hold Cypress harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of Cypress products.

Cypress, the Cypress logo, Spansion, the Spansion logo, and combinations thereof, WICED, PSoC, CapSense, EZ-USB, F-RAM, and Traveo are trademarks or registered trademarks of Cypress in the United States and other countries. For a more complete list of Cypress trademarks, visit cypress.com. Other names and brands may be claimed as property of their respective owners.