Advanced Sector Protection (ASP) in Quad SPI, Octal SPI, and HyperFlash Device Families

About this document

Scope and purpose

AN98551 describes Advanced Sector Protection (ASP) features in Quad SPI (S25FL-S, S25FS-S, S25HL-T, S25HS-T), Octal SPI (S28HL-T, S28HS-T), and HyperFlash™ (S26KL-S, S26KS-S, S26HL-T, S26HS-T) families.

Table of contents

1 Introduction

The Quad SPI (S25FL-S, S25FS-S, S25HL-T, S25HS-T), Octal SPI (S28HL-T, S28HS-T), and HyperFlash (S26KL-S, S26KS-S, S26HL-T, S26HS-T) families of devices offer many ways to protect the data in the memory. The choices can be overwhelming to users. This document explains the overall data protection mechanisms associated with Advanced Sector Protection (ASP). See the device datasheets for specific commands or registers for information on how to implement ASP functions.

2 Legacy Data Protection

Most SPI flash devices use the same subset of core commands for backward compatibility. Within this group of legacy commands and features for data protection, Block Protection Bits (BP Bits), and the WP# pin are common methods of sector protection.

In systems where multiple flash vendors' devices are used, it may be desirable to use the commands or features that work across all devices. When it comes to protecting sectors in SPI flash, the BP Bits are the common way to do it. This method allows you to protect the full array, half the array, a quarter of the array, etc. The WP# pin is also a common way to provide hardware protection.

The Quad SPI flash family maintains this compatibility by providing the BP Bits and the WP# pin. The Octal SPI family provides only the BP Bits, not the WP# pin function.

The HyperFlash family mostly conforms to Parallel NOR flash command sets. Consequently, it does not provide the BP bits or the WP# pin function.

Table 1 summarizes the legacy protection features supported by these families.

Table 1 Legacy Protection Features

	Block Protection Bits	WP# pin (Hardware Protection)
Quad SPI (S25)	Yes	Yes
Octal SPI (S28)	Yes	No
HyperFlash (S26)	No	No

3 Advanced Sector Protection (ASP)

ASP features were first introduced in Parallel NOR devices; these have been incorporated into the SPI flash family, now into the Quad SPI, Octal SPI and HyperFlash families. These features offer greater resolution for protecting sectors.

At the basic level, the ASP is quite simple. Any sector can be protected from being programmed or erased. Such protection can be done by either the Dynamic Protection Bits (DYB), or the Persistent Protection Bits (PPB). Thus, these two methods are called DYB Protection, or PPB Protection.

3.1 DYB Protection

DYB Protection provides a quick way to turn protection ON and OFF. Each sector is associated with a DYB bit. You can set the bit to 0 or 1 by a simple write command corresponding to the protected state or unprotected state. The value of the DYB bits will be reset upon power cycle, typically in unprotected state, i.e. Value 1.

You can individually set any DYB bit to 0 to protect a sector or to 1 to unprotect a sector with the DYB Write command, which uses the provided address to determine the DYB bit to set. DYB Protection is ideal for sectors that are meant to be frequently protected and unprotected.

Because DYB bits are implemented in RAM, they are simple to use. They do not have to be erased as a group and they do not wear out. Additionally, DYB bits accept new values immediately. There is no waiting time associated with the write command.

3.2 PPB Protection

Use PPB protection to have the sector protection status maintained after power cycles. PPB bits are an array of bits stored in flash memory cells. Each bit in the array protects one sector. If a PPB bit is 0 (in the programmed state), the corresponding sector is protected.

You can individually program PPB bits (make the bit to 0) to protect a sector with the PPB Program command. The command uses the provided sector address to determine the associated PPB bit to be programed. Because PPB bits are in the flash, programming is not instant. You must wait for the programming operation to complete, just like when a normal memory program command is executed.

To unprotect a sector that is protected by a PPB bit, change the bit to 1 with the PPB Erase command, not the program command. That means the full array of the PPB bits will be erased to 1. You must then program some PPB bits back to 0 to protect sectors that still need PPB protection. Note that there would be waiting period in this process when all sectors are unprotected by PPB after the PPB Erase command. Therefore, such operation needs to be executed with caution.

The group of PPB bits resides in a small sector of flash, called the PPB array. As with all flash sectors, they also have the same endurance and retention limit as other memory cells. There is a limit to the number of times you can program and erase the PPB array. If every program and erase operation of the normal flash space begins with a PPB Erase and ends with a PPB Program, the PPB array will wear out long before the rest of the array. Therefore, PPB usage should be limited to protecting flash data that does not change often, such as code storage.

In addition to the basic protection method with PPB bits, additional logic is necessary to prevent malicious software from changing the code or causing a denial of service.

4 Protection Modes

4.1 PPB Lock Bit

The PPB Lock Bit is located in the PPB Lock Register. It is used to enable/disable alterations to the PPB Array. When the PPB Lock Bit is 0, the PPB Array is protected; changing any PPB bit value is prevented. That means you cannot unprotect sectors protected with PPB, and you cannot protect unprotected sectors with PPB.

The PPB Lock Bit is set to 0 (PPB Array protected) at power on in the Password Protection Mode. Setting Password Protection Mode is described below. The software must issue a Password Unlock command to set the PPB Lock Bit to 1 so PPB bits can be changed. The PPB Lock Bit is set to 0 at the next reset/power cycle. This is Infineon most secure boot mode. Using this method ensures that protected sectors cannot be changed without a password.

The PPB Lock bit is set to 1 (PPB Array unprotected) at power on in Persistent Protection Mode. Setting Persistent Protection Mode is described below. The software can lock the PPB Lock bit (change it to 0) with the PPB Lock Bit Write command, but doing so will lock the PPB Lock Bit until the next hardware reset or power cycle. There is no command to set the PPB Lock Bit to 1 (unprotect the PPB Array). It can only be reset by hardware reset or power cycle.

4.2 Two Protection Modes

There are two protection modes the user can choose from: Persistent Protection or Password Protection. The protection mode determines how the PPB Lock Bit behaves at power on and after hardware reset. Choose the protection mode to use by programming the one-time programmable bit in the ASP Register. The default protection mode of the device is Persistent Protection.

If you want to use Persistent Protection Mode, it is still recommended to select it during your manufacturing process. Failure to do so will enable malicious software to set Password Protection Mode. Then the malicious software will know the password and be able to change flash code/data. Once the Protection Mode has been selected, it cannot be changed.

The register used to set protection modes is called ASP Register. This is a One-Time-Programmable (OTP) register. Refer to the corresponding flash family datasheet for specific command to program bits in this register. Since this register resides in flash, programming is not instant. It is necessary to wait for the programming operation to complete. Refer to the corresponding datasheet for the command sequences. Infineon provides a Low Level Driver (LLD) written in C which can be used for code or for example how to code. Infineon recommends using the LLD code as a guide.

- Persistent Protection Mode – This mode causes the flash to power up or hardware reset to the PPB Lock bit being 1 (PPB Array unprotected). The user may want the ability to modify PPB bits after power on/reset and then have the boot program or the application lock the PPB Array to prevent changes to the PPB Array and associated protected sectors. The PPB Lock Bit is locked with the PPB Lock Bit Write command, but can only be unlocked by hardware reset/power cycle as there is no command to set the PPB Lock Bit to 1 (unprotect the PPB Array).
- Password Protection Mode – This mode causes the flash to power up or hardware reset to the PPB Lock Bit being 0 (PPB Array protected). This prohibits changes to the PPB array. To unlock the PPB Lock Bit, the software must send the Password Unlock command with the appropriate password. Then the PPB Lock Bit will change to 1 and remain unlocked until the next hardware reset, power cycle or a PPB Lock Bit Write command. This is the most secure data protection mode in these devices. Using this method ensures that protected sectors cannot be changed without a password. When setting up the Password Protection Mode in the device, users need to do the following:

1. Program a password and verify it.
2. Set the Password Protection Mode bit in the ASP register.

Note: *If the system inadvertently programs or erases a protected sector, the Status Register will show error status. The system is then required to clear the error status before any other command can be issued.*

5 Read Password Protection

Read Password Protection works similarly as the normal Password Protection mode but adds a read protection function. When this mode is enabled, upon POR, only the lowest or highest address range, selected by a configuration register, can be read. All other memories are not readable until the correction passwords are entered. The full memory is protected from being erased or programmed as well before entering the correct passwords.

Typically, it is an ordering option to get devices that provide Read Password Protection. For S25FL-S and S25FS-S families, contact the factory for availability.

6 Permanent Protection

In 45-nm Quad SPI and Octal SPI families, the PPBOTP bit in the ASP register provides the option to disable modification of PPB Array. If this bit is set, PPB protection becomes permanent. You can no longer program or erase any PPB bits. This bit itself is an OTP (One Time Programmable) bit.

For 65-nm Quad SPI families, S25FL-S and S25FS-S, contact the factory for availability of this function.

7 DYB Lock Boot

In 45-nm Quad SPI and Octal SPI families, the DYBLBB bit in the ASP register provides the option to set all DYB bits to protected state upon POR, Hardware Reset or Software Reset. When this bit is set, instead of coming up with all unprotected state, all DYB bits will be in protected state so all sectors are protected by DYB protection. The user will need to clear the corresponding DYB bits before trying to program or erase a sector.

For 65-nm Quad SPI families, S25FL-S and S25FS-S, contact the factory for availability of this function.

8 Summary

The Quad SPI, Octal SPI, and HyperFlash families of devices offer Advanced Sector Protection feature that can be used to protect data in different levels. DYB Protection provides an easy, quick protection to any sectors in the device. PPB Protection provides a non-volatile protection to any sectors. You can also use Password Protection or Persistent Protection Mode to alter the power-on behavior of the PPB Lock Bit. Detail operations of all these functions are different in each device families. Refer to the specific datasheet for operational details.

9 Software Support

Infineon provides software Low Level Driver (LLD) that implements the aforementioned functions. The LLD, along with other software and tools, are available for download on this page (Software & Tools tap): **https://www.cypress.com/products/serial-nor-flash-memory**.

References

[1] **001-98283: S25FL128S, S25FL256S Datasheet**

[2] **002-00368: S25FS128S, S25FS256S Datasheet**

[3] **001-99198: S26KL-S, S26KS-S Datasheet**

[4] 002-12345: Semper S25HL-T and S25HS-T Quad SPI Datasheet

[5] 002-12337: Semper S26HL-T and S26HS-T HyperBus Interface Datasheet

[6] 002-18216: Semper S28HL-T and S28HS-T Octal SPI Datasheet

[7] 002-12340: Semper 2Gb and 4Gb Quad SPI MCP Datasheet

[8] 002-23793: Semper 2Gb and 4Gb HyperBus MCP Datasheet

[9] 002-23755: Semper 2Gb and 4Gb Octal SPI MCP Datasheet

Revision history

Document version	Date of release	Description of changes
**	2012-12-10	Initial version
*A	2015-09-21	Updated in template
*B	2017-08-29	Updated logo and copyright
*C	2017-09-26	Major update to include other flash families
*D	2019-11-06	Updated Semper Flash Part Numbers Added section Software Support Updated References section Completing Sunset Review
*E	2021-03-25	Updated to Infineon template

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2021-03-25
Published by
Infineon Technologies AG
81726 Munich, Germany

Do you have a question about this document?
Go to www.cypress.com/support

Document reference
001-98551 Rev. *E

IMPORTANT NOTICE
The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS
Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.