AN200452

Cypress Advanced Sector Protection

AN200452 describes the implementation of the Advanced Sector Protection in Cypress flash memory devices.

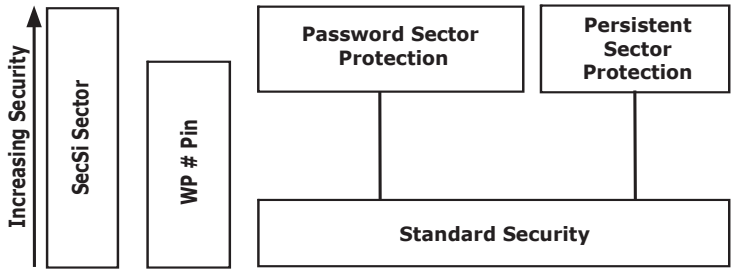
1 Introduction

This document describes the implementation of the Advanced Sector Protection in Cypress flash memory devices. Advanced Sector Protection offers designers multiple levels of sector protection to satisfy a variety of security and design needs. It protects the memory from erroneous codes, accidentally corrupting vital code and data. It also prevents hackers from corrupting the network by programming malicious viruses into the memory.

2 Advanced Sector Protection

Advanced Sector Protection features several levels of sector protection. The scheme is divided into two parts. The Persistent Sector Protection method replaces the 12 V, or V_{ID}, applied on the RESET# pin to initiate sector protect and unprotect. The Password Sector Protection method is a one-time programmable scheme where a 64-bit Password has to be entered for any subsequent programming of a sector. Cypress flash memory devices also have other types of sector protection such as SecSi sector, WP# pin and Standard Security.

Figure 1. Cypress Sector Protection



2.1 Selecting a Sector Protection Mode

All Cypress devices with Advanced Sector Protection default to the Persistent Sector Protection mode. The customer has to make a selection between Persistent and Password Protection. If the customer decides to continue using the Persistent Sector Protection method, they must set the Persistent Sector Protection Mode Locking Bit. This will permanently set the part to operate only in Persistent Sector Protection. If they want to use the Password Protection mode, they have to set the Password Mode Locking Bit. This will set the part permanently only in Password Sector Protection. It is not possible to switch between the two methods once a locking bit has been set. It is important that one mode is clearly selected when the device is first programmed.

The device is shipped with all sectors unprotected. It is possible to determine whether a sector is protected or unprotected by reading sector lock status through Autoselect Command Sequence.

2.2 Persistent Sector Protection

The Persistent Sector Protection method is implemented on a flash memories internal state machine. It replaces the 12 V controlled protection method while at the same time enhancing flexibility by providing three different sector protection states: Persistently Locked, Dynamically Locked, and Unlocked.

The security bits to be manipulated to achieve these states include the Persistent Protection Bit (PPB), Persistent Protection Lock Bit (PPB Lock Bit), and Dynamic Protection Bit (DYB). PPB bits are non-volatile bits that are assigned to each sector or each sector group. The PPB Lock Bit globally locks all PPB bits when it is set with only one PPB Lock Bit per device. The DYB bits are volatile bits with one assigned to each sector or each sector group.

Table 1. Sector Protection Scheme

Protection States			Sector State
DYB Bit	PPB Bit	PPB Lock Bit	
Unprotect	Unprotect	Unfreeze	Unprotected – PPB and DYB are changeable
Unprotect	Unprotect	Freeze	Unprotected – PPB not changeable, DYB is changeable
Unprotect	Protect	Unfreeze	Protected – PPB and DYB are changeable
Unprotect	Protect	Freeze	Protected – PPB not changeable, DYB is changeable
Protect	Unprotect	Unfreeze	Protected – PPB and DYB are changeable
Protect	Unprotect	Freeze	Protected – PPB not changeable, DYB is changeable
Protect	Protect	Unfreeze	Protected – PPB and DYB are changeable
Protect	Protect	Freeze	Protected – PPB not changeable, DYB is changeable

Table 1 contains all possible combinations of the DYB, PPB, and PPB Lock relating to the status of the sector. If the PPB is set, and the PPB Lock is set, the sector is protected and the protection can not be removed until the next power cycle clears the PPB Lock. If the PPB is cleared, the sector can be dynamically locked or unlocked. The DYB bit can be set through the DYB Write Command.

DYB bits are cleared upon power up or hardware reset. Therefore sectors are not protected during power up. PPB Lock bit is cleared upon power up or hardware reset when the device is permanently set to persistent mode.

By default, the Persistent Sector Protection method is always used. To set the device to Persistent Sector Protection permanently, the Persistent Sector Protection Mode Locking Bit must be set. It is not possible to switch to the Password Sector Protection method once the Persistent Sector Protection Locking Bit is set.

Figure 2. Setting Protection Bit in Persistent Mode

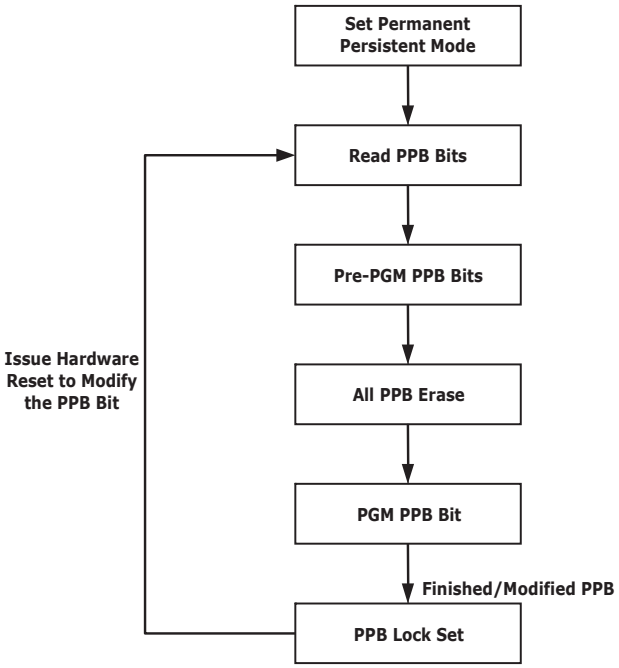
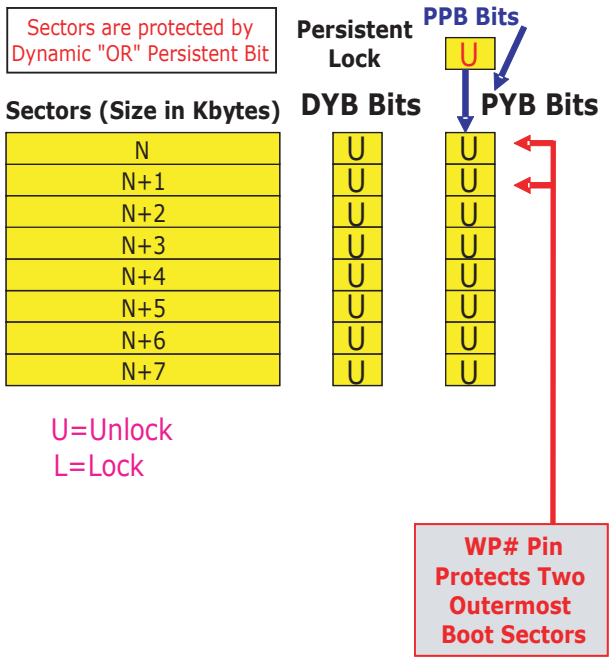


Figure 3. Persistent Sector Protection Mode



2.3 Password Sector Protection

The Password Sector Protection is also implemented on a state machine. The Password Sector Protection method allows an even higher level of security than the Persistent Sector Protection method. The Password Sector Protection method is similar to Persistent Protection except a 64-bit password is added in this method. The Password Sector Protection has four security bits. They are Persistent Protection Bit, Persistent Protection Bit Lock, Dynamic Protection Bit and Password Protection Mode Lock Bit.

The password is stored in a one-time programmable (OTP) region outside of the flash memory. To set the device to Password Protection Mode permanently, the Password Protection Mode Lock Bit must be set. Once set, the password is permanently set with no means to read, program, or erase it. Also, it is not possible to switch to the Persistent Sector Protection method once the Password Protection Mode Lock Bit is set.

The 64-bit password is located in its own memory space and is accessible through the use of the Password Program and Password Read commands. The password function works in conjunction with the Password Protection Mode Lock Bit, which when programmed, prevents the Password Read command from reading the contents of the password.

The password is used to clear and unfreeze the PPB Lock Bit. The Password Unlock command must be written to the flash, along with a password. The flash device internally compares the given password with the pre-programmed password. If they match, the PPB Lock Bit is cleared to the “unfrozen state”, and the PPB bits can be altered. If they do not match, the flash device does nothing. There is a built-in 1 µs delay for each “password check” in password sector protection mode. This delay is intended to thwart any efforts to run a program that tries all possible combinations in order to crack the password.

Command		Cycles	Bus Cycles											
			First		Second		Third		Fourth		Fifth		Sixth	
			Addr	Data	Addr	Data	Addr	Data	Addr	Data	Addr	Data	Addr	Data
Password	Password Protection Command Set Entry	3	555	AA	2AA	55	555	60						
	Password Program	2	XXX	A0	PWAX	PWDX								
	Password Read	4	XXX	PWD0	01	PWD1	02	PWD2	03	PWD3				
	Password Unlock	7	00	25	00	03	00	PWD0	01	PWD1	02	PWD2	03	PWD3
			00	29										
	Password Protection Command Set Exit	2	XXX	90	XXX	00								
Non-Volatile Sector Protection Command Set Definitions														
PPB	Non-Volatile Sector Protection Command Set Entry	3	555	AA	2AA	55	555	C0						
	PPB Program	2	XXX	A0	SA	00								
	All PPB Erase	2	XXX	80	00	30								
	PPB Status Read	1	SA	RD(0)										
	Non-Volatile Sector Protection Command Set Exit	2	XXX	90	XXX	00								
Global Volatile Sector Protection Freeze Command Set Definitions														
PPB Lock Bit	Global Volatile Sector Protection Freeze Command Set Entry	3	555	AA	2AA	55	555	50						
	PPB Lock Bit Set	2	XXX	A0	XXX	00								
	PPB Lock Status Read	1	XXX	RD(0)										
	Global Volatile Sector Protection Freeze Command Set Exit	2	XXX	90	XXX	00								
Volatile Sector Protection Command Set Definitions														
DYB	Volatile Sector Protection Command Set Entry	3	555	AA	2AA	55	555	E0						
	DYB Set	2	XXX	A0	SA	00								
	DYB Clear	2	XXX	A0	SA	01								
	DYB Status Read	1	SA	RD(0)										
	Volatile Sector Protection Command Set Exit	2	XXX	90	XXX	00								

Figure 4. Password Sector Protection

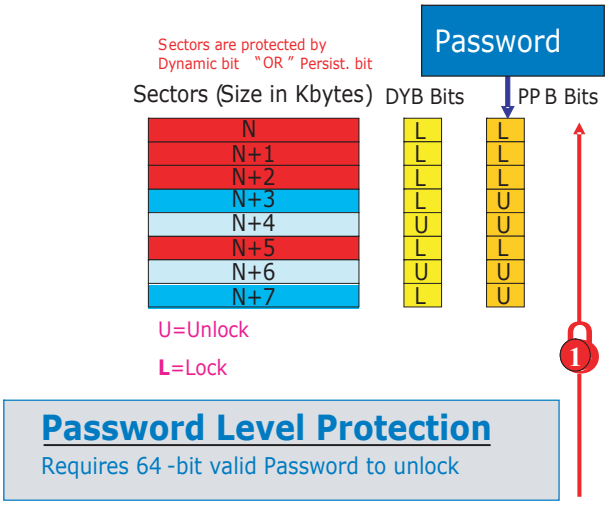
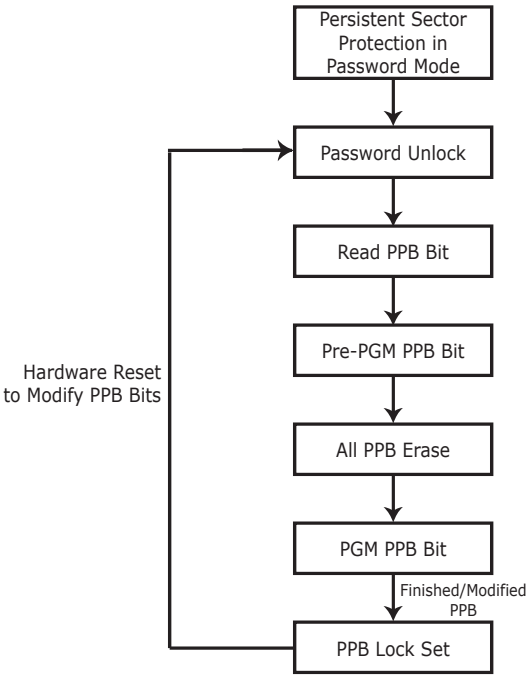


Figure 5. Persistent Sector Protection in Password Mode

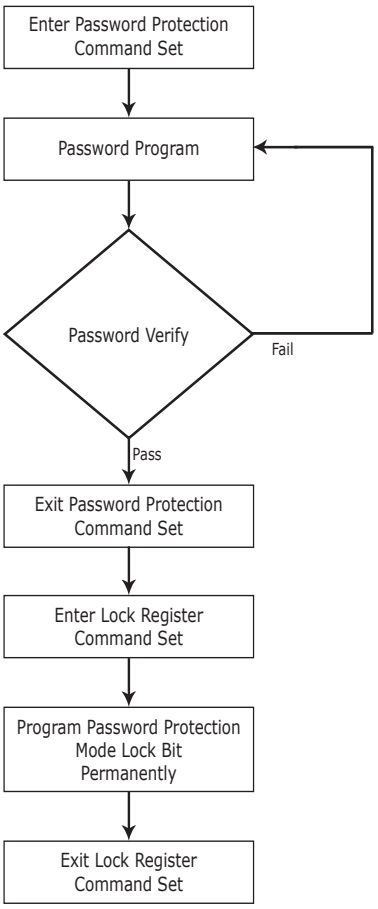


It is recommended that if the user wanted to modify the states of the PPB bits they must read all the PPB bits and shadow the content into RAM. Now the user can Pre-PGM all unprotected PPB bit to the protected state. Once the Pre-PGM of the PPB bits are completed then the user can issue the All PPB erase command to erase all the PPB bits into the unprotected state. The user the can copy back the content from RAM to program the necessary PPB bits the user choose to protect.

2.4 Steps to Set into Password Sector Protection

To choose the Password Sector Protection method, the customer must first program the password. It is recommended that the password be somehow correlated to the unique Electronic Serial Number (ESN) of the particular flash device. Each ESN is different for every flash device; therefore each password should be different for every flash device. While programming in the password region, the customer may perform Password Read operations. The flash device compares the password. If they match, the device is set to Password Mode permanently by programming the Password Protection Mode Lock Bit in the Lock Register.

Figure 6. Set Password Sector Protection



3 Other Security Features

3.1 Secured Silicon Sector

Cypress's Sector Protection also includes the Secured Silicon sector which can be programmed permanently with an Electronic Serial Number (ESN) to defend against cloning and signal theft. The Secured Silicon Sector is 256 bytes in length, and uses a Secured Silicon Sector Indicator Bit (DQ7) to indicate whether or not the Secured Silicon Sector is locked when shipped from the factory.

3.1.1 Write Protect (WP#)

The Write Protect pin provides a hardware method of protecting the first or last sector group without using high voltage (V_{ID}). It adds a final level of hardware protection that could override the choices made while setting up sector protection during system initialization. When this pin is low it is not possible to change the contents of the WP# protected sectors. These sectors generally hold system boot code. So, the WP# pin can prevent any changes to the boot code.

3.2 Standard Security

The Standard Security is the basic protection against system noise, voltage glitches, inadvertent writes, and erroneous code.

4 Conclusion

Cypress's Advanced Sector Protection is the best defense against security threats. It gives customers total control over system security. In addition, it operates at V_{CC} level, thereby lowering power consumption and reducing the design time.

Document History Page

Document Title: AN200452 - Cypress Advanced Sector Protection Document Number: 002-00452				
Rev.	**ECN No.**	**Orig. of Change**	**Submission Date**	**Description of Change**
**	–	–	09/16/2005	Initial version
*A	4958538	MSWI	10/12/2015	Updated in Cypress template
*B	5821086	AESATMP8	07/17/2017	Updated logo and Copyright.

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
198 Champion Court
San Jose, CA 95134-1709