



HT32_ICP TOOL User Guide

Revision: V1.00 Date: August 04, 2023

www.holtek.com

Table of Contents

1. Introduction and Installation	3
1.1 Introduction	3
1.2 Installation	3
2. Quick Start.....	3
3. Functional Introduction.....	4
3.1 Menu Bar.....	4
3.2 Device Connection	6
3.3 Memory Read Setting	7
3.4 Program File Information.....	8
3.5 Erase Function	9
3.6 SPIM Config External Memory Setting.....	10
3.7 sLib Status	11
3.8 User System Data	11
3.9 Access Protection.....	13
3.10 Flash CRC Calculation Function	14
3.11 Download Function.....	14
3.12 SPIM External Memory Encryption Download	19

1. Introduction and Installation

1.1 Introduction

The e-Link32 Pro ICP Tool is a programming software for the HT32 series MCUs, it allows users to update the program memory without removing the target MCU in the PCB. Using this application, users must use the e-Link32 Pro/Lite emulator to operate the HT32 MCU device.

1.2 Installation

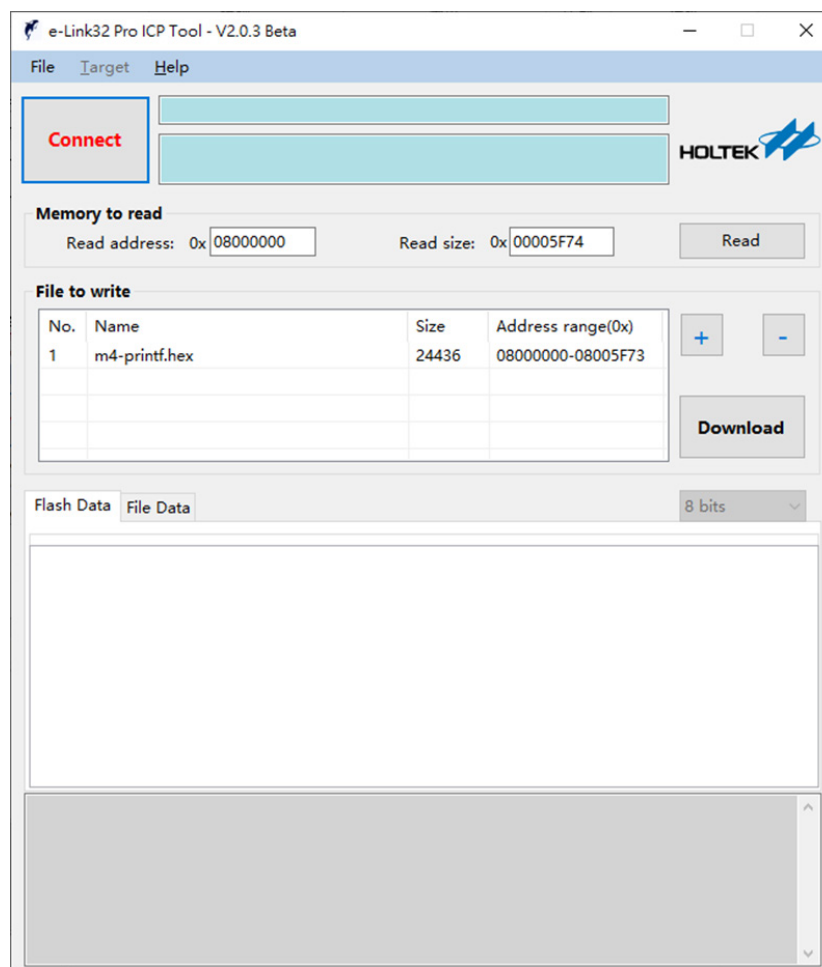
- Install in Microsoft Windows 7/8/10/11 desktop operating systems
- .NET Framework 4 or later must be installed in the system. For Windows 10/11, the software should have already been installed with the system. If it has not been installed, it can be downloaded from the Microsoft website: <https://dotnet.microsoft.com/download>
- During the installation process, keep clicking “Next” as prompted to complete the installation

2. Quick Start

- Connect the HT32 MCU to the computer using the e-Link32 Pro/Lite emulator
- Open the software e-Link32 Pro ICP Tool, click Connect
- Add the hex or bin file to be programmed in the File to write screen
- Click Download, the download screen will be displayed
- Set options, click Start to start the programming
- Wait for the programming to complete

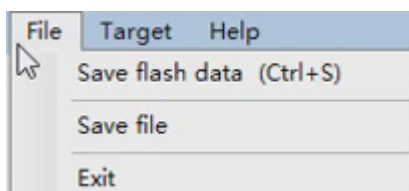
3. Functional Introduction

In this chapter, the basic operations of the tool will be introduced in detail, the main screen is shown below:



3.1 Menu Bar

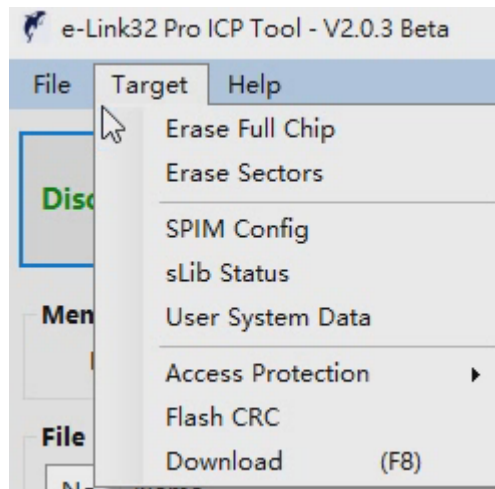
“File” menu:



- Save file: Save the data in the “Download file information” table as a file. Supports *.bin/*.hex format.
- Save flash data: Save the flash memory data in the “Flash data” table as a file. Supports *.bin/*.hex format.
- Exit: Exit the software.

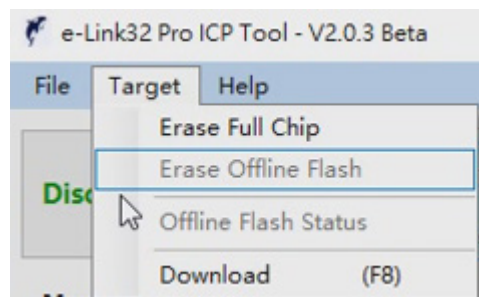
“Target” menu: The function content is different when connecting to HT32 M0+/M3 series and HT32 M4 series.

Menu when connecting to HT32 M4:



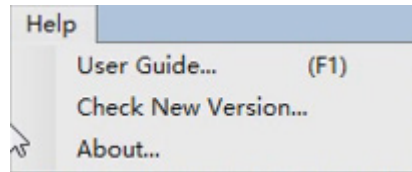
- Erase Full Chip: Erase the full chip main memory.
- Erase Sectors: User selects the sector to be erased to erase.
- SPIM Config: External memory setting
- User System Data: User system data setting, including access and erase and program protection, etc.
- Access Protection: Enable access protection and disable access protection.
- sLib Status: Check the sLib current status, and is able to disable the sLib.
- Download: Set the download option and downloads the file to the memory.
- Flash CRC: Calculate the CRC value for the selected memory sector range.

Menu when connecting to HT32 M0+/M3 series:



- Erase Full Chip: Erase the full chip main memory.
- Erase Offline Flash: Erase the offline flash memory (e-Link32 Lite hardware does not support this function, the menu is gray)
- Offline Flash Status: Offline flash memory status (e-Link32 Lite hardware does not support this function, the menu is gray)
- Download: Set the download options and download the file to the memory.

“Help” menu:



- User Guide...: Open the user guide of this software.
- Check New Version...: Check if there is a new available version of ICP software, if so, download the new ICP version. The computer needs to be connected to the internet.
- About...: Release Notes information screen.

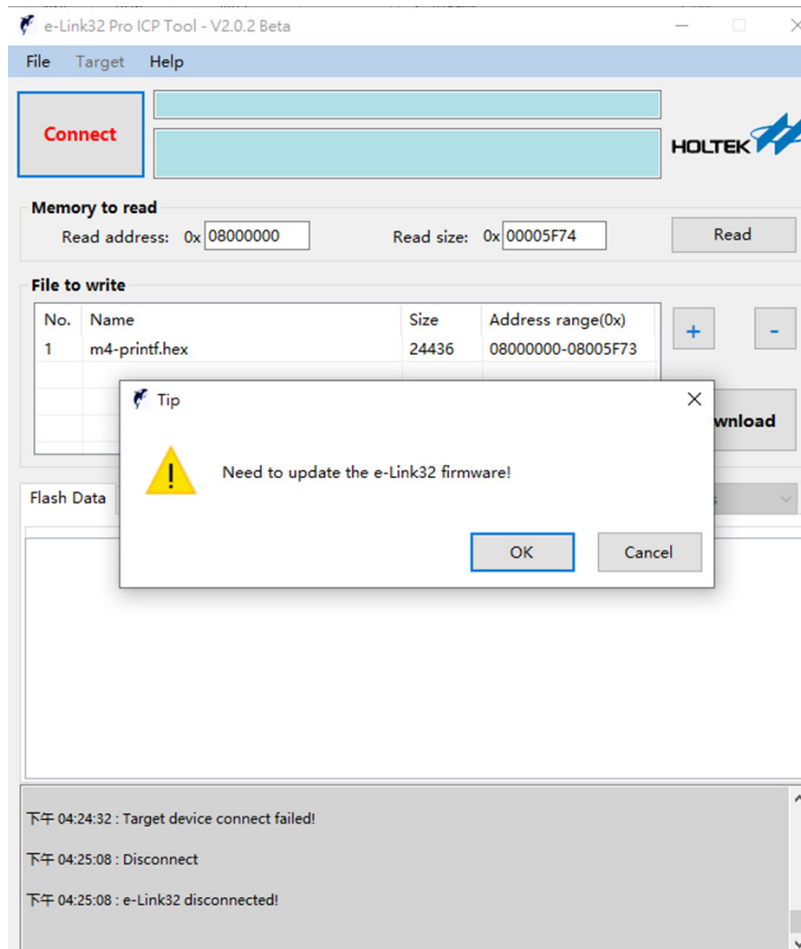
3.2 Device Connection

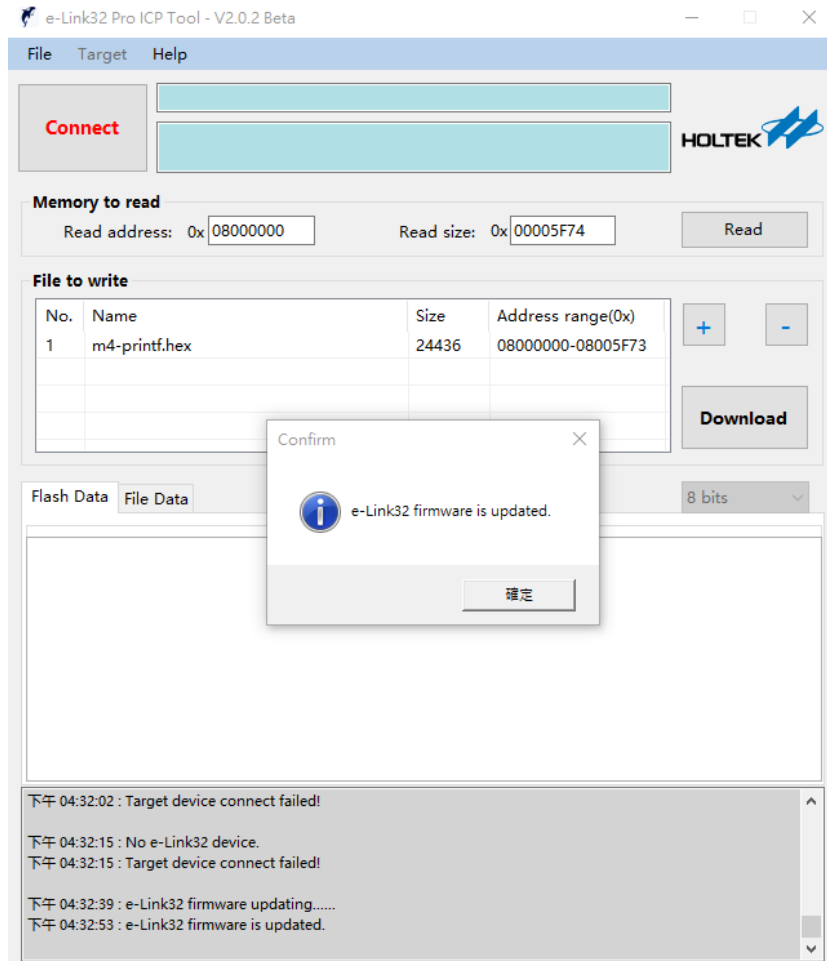
Before connection-No recognized device at this time. As shown below:

Click “Connect”, if the e-Link32 firmware version is lower, it will prompt to upgrade the firmware.



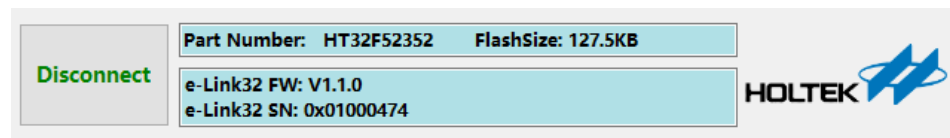
Click “OK” to update.





Click “Connect” to connect the device.

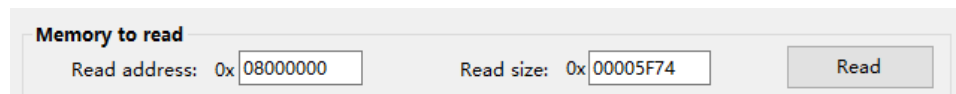
After successful connection-Identify the device correctly. As shown below:



After the device is successfully connected, the e-Link32 relevant information will be displayed, including e-Link32 type, e-Link32 series number etc. The MCU relevant information will also be displayed, including MCU type and main flash memory size.

Click “Disconnect” to disconnect from the device.

3.3 Memory Read Setting



Read address: Start address of the memory to read.

Read size: Size of the memory to read

Flash Data

Download File Info

8 bits

Address range:[0x08000000 0x08005F73] checksum: 0x00230109

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x08000000	80	19	00	20	39	02	00	08	3B	0B	00	08	41	08	00	08
0x08000010	37	0B	00	08	05	07	00	08	E1	1E	00	08	00	00	00	00
0x08000020	00	00	00	00	00	00	00	00	00	00	00	00	BD	1D	00	08
0x08000030	09	07	00	08	00	00	00	00	3D	0B	00	08	05	1E	00	08
0x08000040	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08
0x08000050	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08
0x08000060	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08

3.4 Program File Information

Display the file information to be downloaded, including file name, file size, download location, etc.
Supports *.bin and *.hex file formats. As shown below:

File to write					
No.	Name	Size	Address range(0x)		
1	m4-printf.hex	24436	08000000-08005F73		
				Download	

Add

Add the file to be downloaded to the download list. And display the file data in the “File to write” table. Supports up to 5 files.

After the file is successfully opened, the file content will automatically be displayed in the “File to write” table, as shown below:

Flash Data

File:m4-printf.hex

8 bits

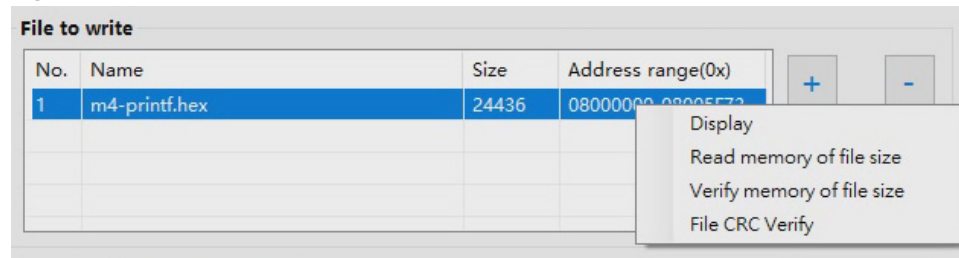
Address range:[0x08000000 0x08005F73] checksum: 0x00230109

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0x08000000	80	19	00	20	39	02	00	08	3B	0B	00	08	41	08	00	08
0x08000010	37	0B	00	08	05	07	00	08	E1	1E	00	08	00	00	00	00
0x08000020	00	00	00	00	00	00	00	00	00	00	00	00	BD	1D	00	08
0x08000030	09	07	00	08	00	00	00	00	3D	0B	00	08	05	1E	00	08
0x08000040	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08
0x08000050	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08
0x08000060	53	02	00	08	53	02	00	08	53	02	00	08	53	02	00	08

Delete

Delete the file in the file list.

Right Click the Menu



Display: Display the content of the selected file in the “File to write” table.

Read memory of file size: Read data of the same size as the selected file from the memory.

Verify memory of file size: Read data of the same size as the selected file from the memory and perform a comparison check for each byte.

File CRC Verify: Select file and corresponding memory data for CRC verification.

3.5 Erase Function

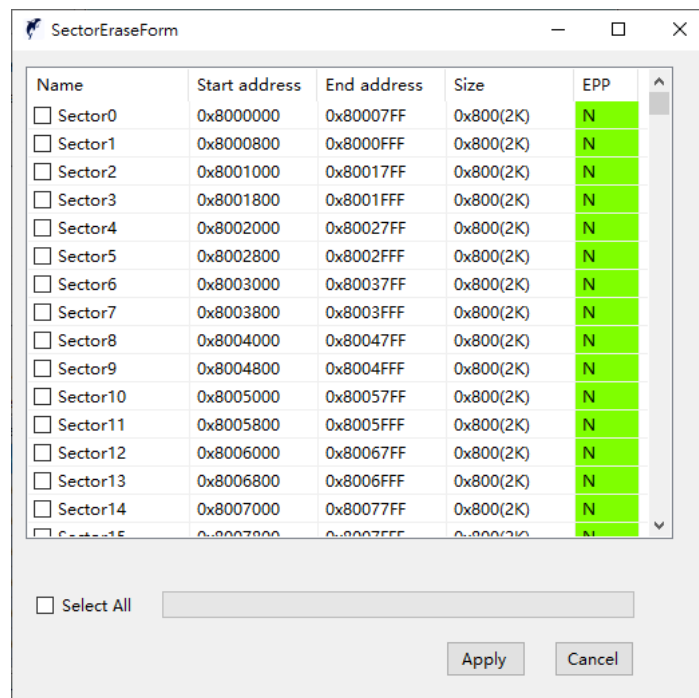
Erase the main memory. (Tool bar → “Target”)

Erase Full Chip

Erase the full chip main memory.

Erase Sector

Erase the user selected sector. “Target” and “Erase Sector” are shown below:



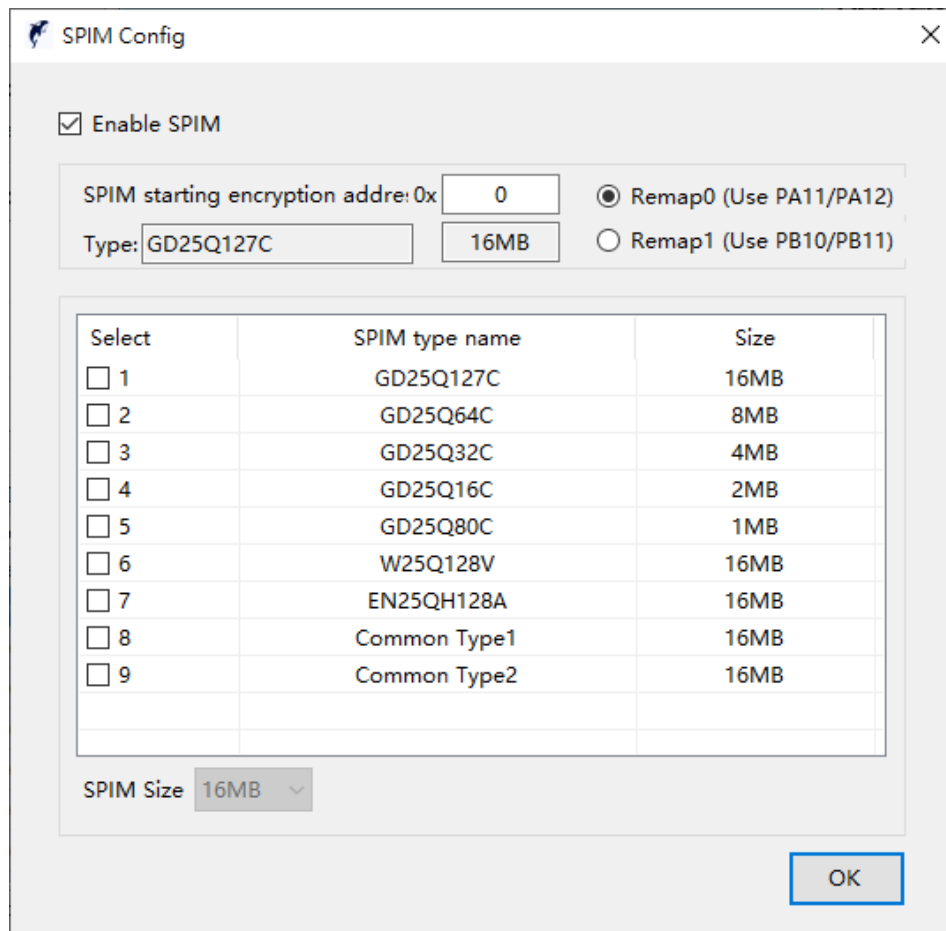
Apply: Erase the selected sector.

Cancel: During the erase process, cancel this erase operation.

3.6 SPIM Config External Memory Setting

Before using the external memory, the external memory must be set, otherwise it will not be able to operate properly.

As shown below:



The SPIM Config dialog box contains the following elements:

- ☒ Enable SPIM
- SPIM starting encryption address: 0x
- Type:
- ☒ Remap0 (Use PA11/PA12)
- ☐ Remap1 (Use PB10/PB11)

Select	SPIM type name	Size
<input type="checkbox"/> 1	GD25Q127C	16MB
<input type="checkbox"/> 2	GD25Q64C	8MB
<input type="checkbox"/> 3	GD25Q32C	4MB
<input type="checkbox"/> 4	GD25Q16C	2MB
<input type="checkbox"/> 5	GD25Q80C	1MB
<input type="checkbox"/> 6	W25Q128V	16MB
<input type="checkbox"/> 7	EN25QH128A	16MB
<input type="checkbox"/> 8	Common Type1	16MB
<input type="checkbox"/> 9	Common Type2	16MB

SPIM Size

OK

Check “Enable SPIM”: External memory operations are available.

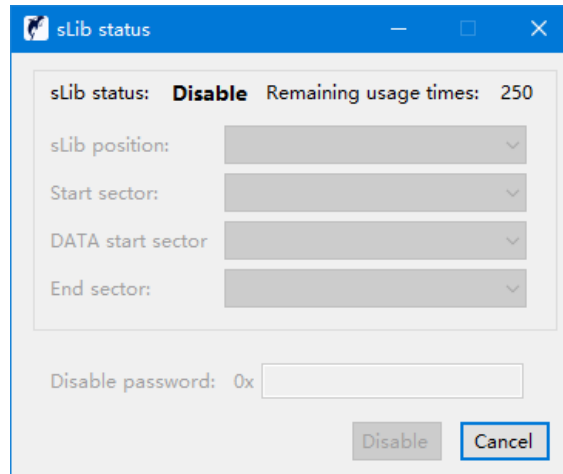
No check “Enable SPIM”: External memory operations are not allowed.

SPIM starting encryption address: Set the encryption range when downloading files to the external memory, calculate the encryption range starting from 0x08400000 address.

Remap 0 (Uses PA11/PA12 pin) / Remap 1 (Uses PB10/PB11 pin): Select external memory connection pin.

Type: There are 9 types for selection

3.7 sLib Status



sLib status: **Disable** Remaining usage times: 250

sLib position:

Start sector:

DATA start sector:

End sector:

Disable password: 0x

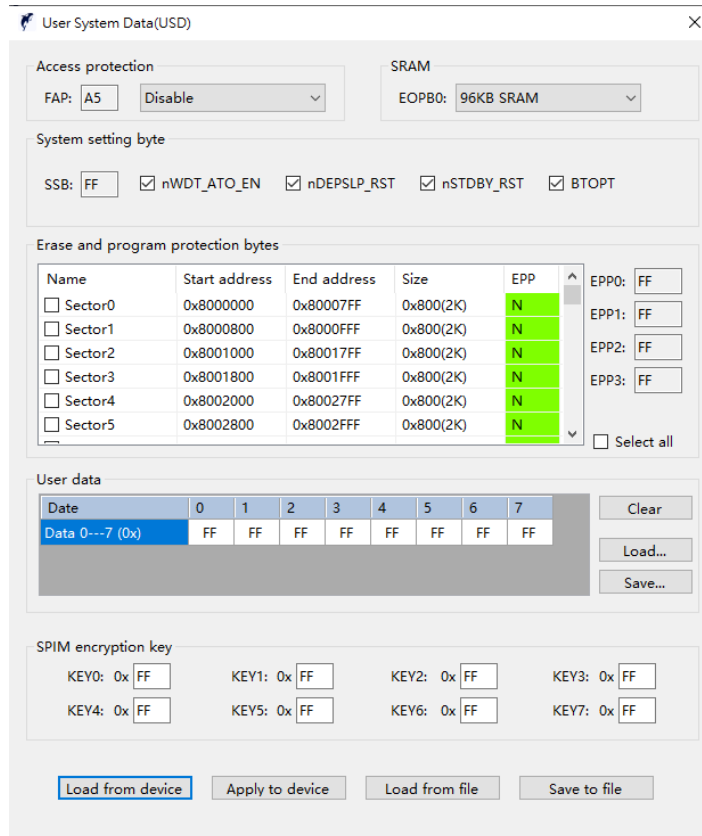
The sLib status is displayed in this page, including whether to enable, remaining usage times, Start sector, DATA start sector, End sector.

If the sLib is enabled, users can enter the correct password in the Disable password input box to turn off the sLib.

Note: Disabling sLib will cause the full chip to be erased.

3.8 User System Data

Program the user system data, (Tool bar → “Target” → “User System Data”), as shown below:



User System Data(USD)

Access protection
FAP: A5

SRAM
EOPB0: 96KB SRAM

System setting byte
SSB: FF ☒ nWDT_ATO_EN ☒ nDEPSLP_RST ☒ nSTDBY_RST ☒ BTOPT

Erase and program protection bytes

Name	Start address	End address	Size	EPP
<input type="checkbox"/> Sector0	0x8000000	0x80007FF	0x800(2K)	N
<input type="checkbox"/> Sector1	0x8000800	0x8000FFF	0x800(2K)	N
<input type="checkbox"/> Sector2	0x8001000	0x80017FF	0x800(2K)	N
<input type="checkbox"/> Sector3	0x8001800	0x8001FFF	0x800(2K)	N
<input type="checkbox"/> Sector4	0x8002000	0x80027FF	0x800(2K)	N
<input type="checkbox"/> Sector5	0x8002800	0x8002FFF	0x800(2K)	N

EPP0: FF EPP1: FF EPP2: FF EPP3: FF ☐ Select all

User data

Date	0	1	2	3	4	5	6	7
Data 0---7 (0x)	FF	FF	FF	FF	FF	FF	FF	FF

SPIM encryption key

KEY0: 0x FF KEY1: 0x FF KEY2: 0x FF KEY3: 0x FF
KEY4: 0x FF KEY5: 0x FF KEY6: 0x FF KEY7: 0x FF

Access the Protection Bytes

Enable or disable the memory access protection.

Enable: FAP is 0xFF.

Disable: FAP is 0xA5.

When enabling the access protection, both memory and user system data cannot be read, and the access protection requires to be disabled before operation.

After disabling the access protection, the main memory and user system data will be erased.

System Setting Byte

nWDT_ATO_EN:

No check-Enable watchdog self-starting.

Check-Disable watchdog self-starting.

nDEPSLP_RST:

No check-Reset occurs when entering the deep sleep mode.

Check-No reset occurs when entering the deep sleep mode.

nSTDBY_RST:

No check-Reset occurs when entering the standby mode.

Check-No reset occurs when entering the standby mode.

BTOPT:

No check-When starting from the main flash memory is configured, if there is no startup program in chip 2, it will start from chip 1; otherwise, it will start from chip 2.

Check-When starting from main flash memory is configured, start from chip 1.

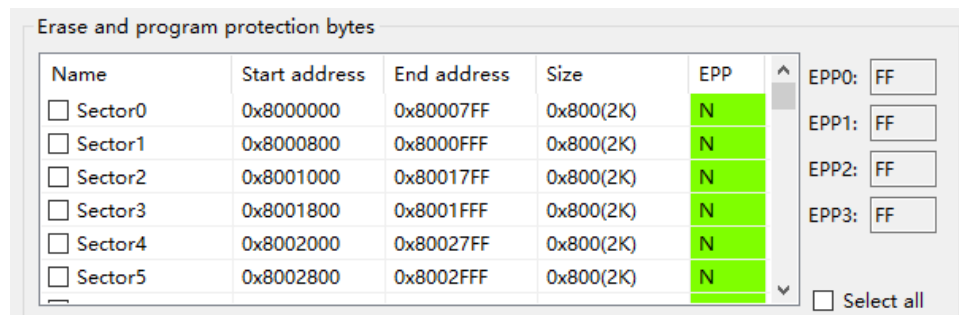
EOPB0 (On-chip memory)

224KB SRAM-On-chip memory 224KB.

96KB SRAM-On-chip memory 96KB.

Erase and Program Protection Bytes

Select the sector that requires write protection. As shown below:



Name	Start address	End address	Size	EPP
<input type="checkbox"/> Sector0	0x8000000	0x80007FF	0x800(2K)	N
<input type="checkbox"/> Sector1	0x8000800	0x8000FFF	0x800(2K)	N
<input type="checkbox"/> Sector2	0x8001000	0x80017FF	0x800(2K)	N
<input type="checkbox"/> Sector3	0x8001800	0x8001FFF	0x800(2K)	N
<input type="checkbox"/> Sector4	0x8002000	0x80027FF	0x800(2K)	N
<input type="checkbox"/> Sector5	0x8002800	0x8002FFF	0x800(2K)	N

EPP0:

EPP1:

EPP2:

EPP3:

☐ Select all

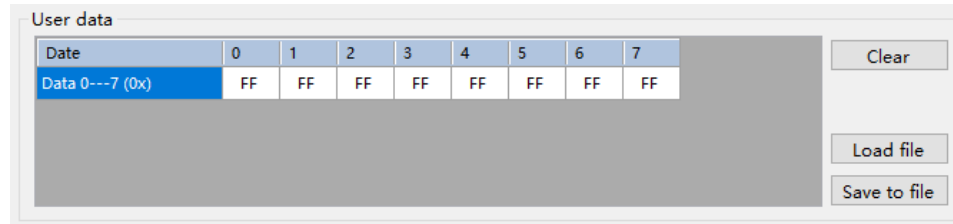
EPP0: Control the erase and program protection of the sector within the range of Flash 1K~32K.

EPP1: Control the erase and program protection of the sector within the range of Flash 33K~64K.

EPP2: Control the erase and program protection of the sector within the range of Flash 65K~96K.

EPP3: Bits 0~6 control the erase and program protection of the sector within the range of Flash 97K~124K. Bit 7 controls the erase and program protection of all the sectors after the Flash 124K, including external memory.

User data



Date	0	1	2	3	4	5	6	7
Data 0---7 (0x)	FF	FF	FF	FF	FF	FF	FF	FF

User data byte: 8 bytes.

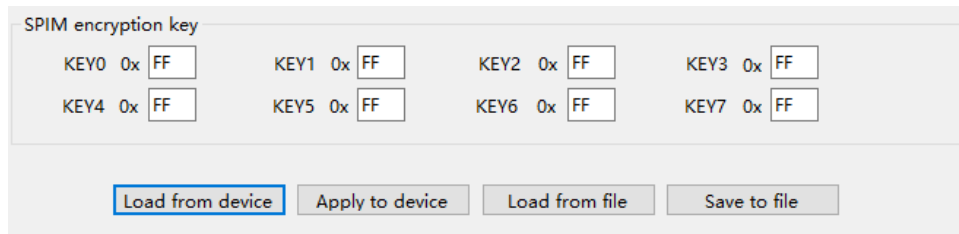
Clear: Reset all user system data to 0xFF, at this time, it has not been saved to the device.

Load file: Import the saved data byte file into the table for display

Save to file: Save the user system data in the table to a file.

SPIM encryption key

Set external memory ciphertext access location encryption key value. As shown below:



KEY0 0x	FF	KEY1 0x	FF	KEY2 0x	FF	KEY3 0x	FF
KEY4 0x	FF	KEY5 0x	FF	KEY6 0x	FF	KEY7 0x	FF

Load from device

Read the user system data content from the device, update and display it to the screen.

Apply to device

Save the user system data setting to the device.

Load from file

Load the saved user system data file content, update and display it to the screen.

Save to file

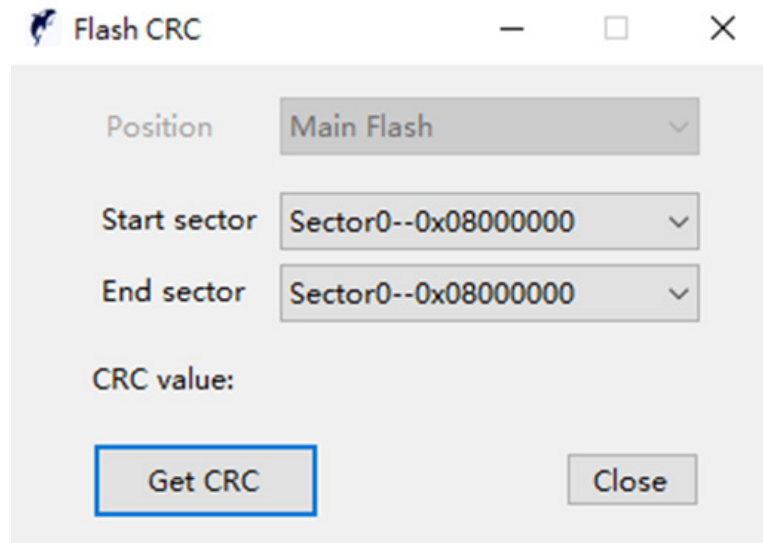
Save the user system data setting to the file.

3.9 Access Protection

Enable is in the Flash Access Protection on status, at this time, the MCU flash content cannot be read using the SWD interface.

Disable is in the Flash Access Protection off status, if the MCU is already in a protected status, the Disable operation will erase full chip.

3.10 Flash CRC Calculation Function



Whether the MCU is in the Access Protection status, the Flash CRC can always get CRC, the minimum calculation unit is sector.

Position: Main Flash

Start sector: Calculate the CRC start sector.

End sector: Calculate the CRC end sector.

CRC value: The calculated CRC value.


Get CRC: Start calculating the CRC value.

Close: Close the dialog.

3.11 Download Function

The “Download option” setting screen can be opened by using “Tool bar” → “Device operation” → “Download”, or using the “Download” button on the main screen. The download setting screens for HT32 M0+/M3 series and HT32 M4 series are different.

As shown below:

 Download
 —
□
×

Option byte

<input checked="" type="checkbox"/> Security Protection	OB_PP0	0x	<input type="text" value="FFFFFFFF"/>
	OB_PP1	0x	<input type="text" value="FFFFFFFF"/>
	OB_PP2	0x	<input type="text" value="FFFFFFFF"/>
<input checked="" type="checkbox"/> Option Byte Write Protection	OB_PP3	0x	<input type="text" value="FFFFFFFF"/>

Download Function

<input checked="" type="radio"/> Erase Full Chip	<input checked="" type="checkbox"/> Program
<input type="radio"/> Erase Sectors	<input checked="" type="checkbox"/> Verify
<input type="radio"/> Do not Erase	<input type="checkbox"/> Reset and Run

☐ Write Serial Number(SN)

Write address:	0x	<input type="text" value="400"/>
Current SN:	0x	<input type="text" value="1"/>
Increase step:	0x	<input type="text" value="1"/>

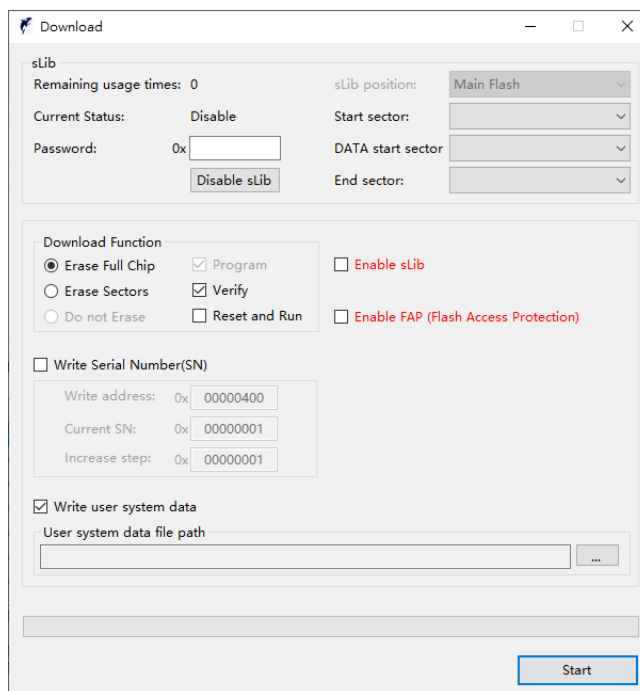
☐ Offline Programming Mode

<input type="checkbox"/> Use Password for Offline Data
Enter Password: <input type="text" value="12345678"/>
<input type="checkbox"/> Limit The Number of Offline Programming
MAX Number: <input type="text" value="1000"/>

CRC16: 26E8

Start

HT32 M0+/M3 Series Download Setting Screen



HT32 M4 Series Download Setting Screen

Option bytes

Set the security protection, users can lock the MCU or select the sectors that require write protection.

sLib Setting

sLib Status

The sLib status of the current connected chip, disable or enable.

Remaining Usage Times

sLib remaining usage times, users can use it up to 256 times, it will decrease after each use. When the number of remaining usage times is 0, the sLib function will not be available.

Password

Password for enabling and disabling sLib function.

Start Sector

sLib sector start sector. From “Start sector” to “DATA start sector” (excluding “DATA start sector”), these sectors are used for Instruction. After enable the sLib, the data in these sectors cannot be erased, written or read.

DATA start sector/Instruction start sector

sLib DATA start sector. From “DATA start sector” to “End sector” (including “End sector”), these sectors are used for DATA. After enable the sLib, the data in these sectors cannot be erased, written or read. When set to “none”, these sectors are set to no data sector.

End Sector

sLib End sector.

Disable sLib

sLib changes from the enable status to disable status, which requires to enter the password from the last time it was enabled. When the sLib is successfully disabled, the full chip will be erased.

Option

Erase Full Chip

Erase Sectors

Do not Erase

Verify

After the download is completed, the corresponding memory content will be read and verified to determine whether the download was successful. If this option is not checked, no read verification will be performed after downloading, making it impossible to determine whether the downloaded content is correct.

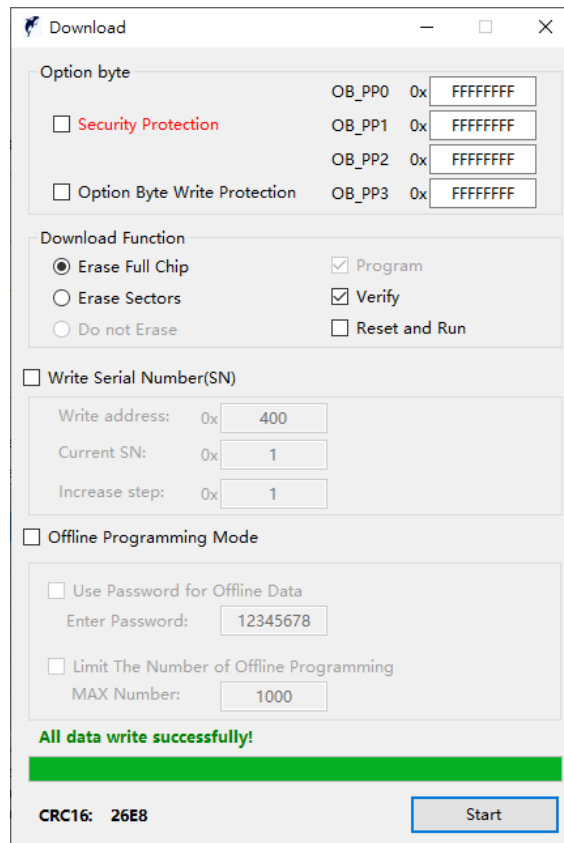
Reset and Run

After the download is completed, the memory address corresponding to the download will be executed.

Enable sLib

Enable the sLib function when downloading. Users need to enter the Password, Start sector, DATA start sector/Instruction start sector and End sector for enabling the sLib this time.

Enable FAP (Flash Access Protection)



Download

Option byte

☐ Security Protection

☐ Option Byte Write Protection

OB_PP0 0x FFFFFFFF

OB_PP1 0x FFFFFFFF

OB_PP2 0x FFFFFFFF

OB_PP3 0x FFFFFFFF

Download Function

☒ Erase Full Chip

☐ Erase Sectors

☐ Do not Erase

☒ Program

☒ Verify

☐ Reset and Run

☐ Write Serial Number(SN)

Write address: 0x 400

Current SN: 0x 1

Increase step: 0x 1

☐ Offline Programming Mode

☐ Use Password for Offline Data

Enter Password: 12345678

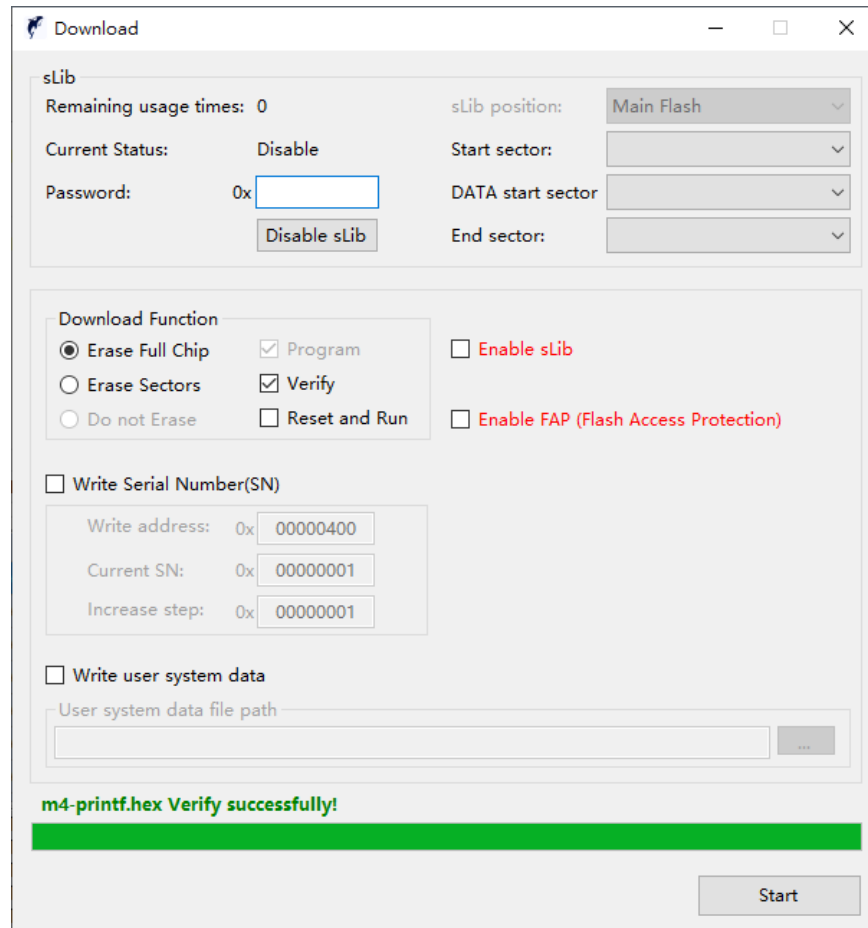
☐ Limit The Number of Offline Programming

MAX Number: 1000

All data write successfully!

CRC16: 26E8

Start

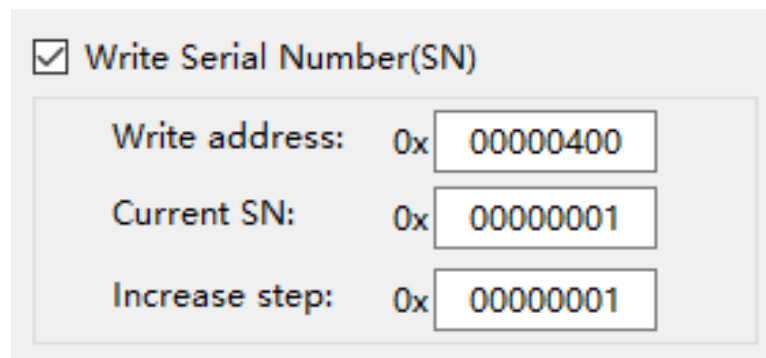


The screenshot shows the 'Download' window of the HT32_ICP TOOL. It contains several sections for configuring the download process:

- sLib Section:** Includes 'Remaining usage times: 0', 'Current Status: Disable', 'Password: 0x' (with a text input field), and a 'Disable sLib' button. It also has dropdown menus for 'sLib position: Main Flash', 'Start sector:', 'DATA start sector:', and 'End sector:'.
- Download Function Section:** Contains radio buttons for 'Erase Full Chip' (selected), 'Erase Sectors', and 'Do not Erase'. It also has checkboxes for 'Program', 'Verify', 'Reset and Run', 'Enable sLib', and 'Enable FAP (Flash Access Protection)'.
- Write Serial Number(SN) Section:** Includes a checkbox for 'Write Serial Number(SN)' and three text input fields for 'Write address: 0x 00000400', 'Current SN: 0x 00000001', and 'Increase step: 0x 00000001'.
- Write user system data Section:** Includes a checkbox for 'Write user system data' and a text input field for 'User system data file path'.
- Status Bar:** Displays a green message 'm4-printf.hex Verify successfully!'.
- Start Button:** A button labeled 'Start' is located at the bottom right.

Write Serial Number (SN)

After the option is selected, the serial number will be automatically written for each device after the program file download is completed. Settings can be made using the screen, as shown below:



This close-up shows the 'Write Serial Number(SN)' section of the tool. It features a checked checkbox and three text input fields:

- Write address:** 0x 00000400
- Current SN:** 0x 00000001
- Increase step:** 0x 00000001

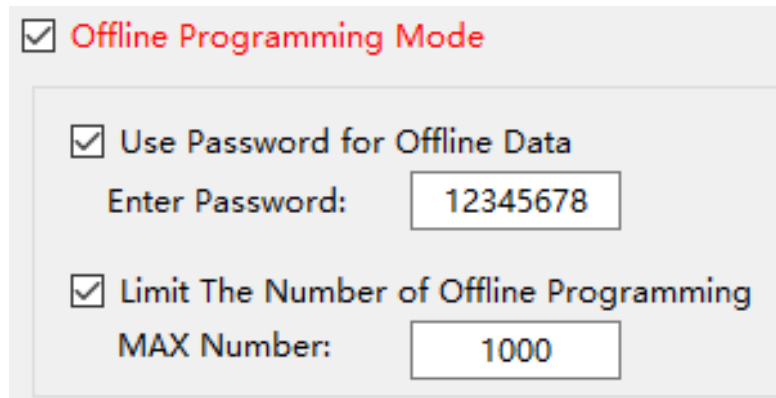
Write address: The memory address that serial number is written in.

Current SN: The serial number written this time.

Increase step: The increment for the next serial number after each serial number programming.

Offline Programming Mode (e-Link32 Lite hardware does not support, this function is gray)

The offline programming mode setting screen allows users to set the read password and the maximum number of offline programming times for the offline programming data.



☒ Offline Programming Mode

☒ Use Password for Offline Data
Enter Password:

☒ Limit The Number of Offline Programming
MAX Number:

Write user system data

After this option is selected, user system data can be automatically programmed to the device after downloading the program files and programming the serial number.

Users can implement the settings using the screen, as shown below:



☒ Write user system data

User system data file path ...

3.12 SPIM External Memory Encryption Download

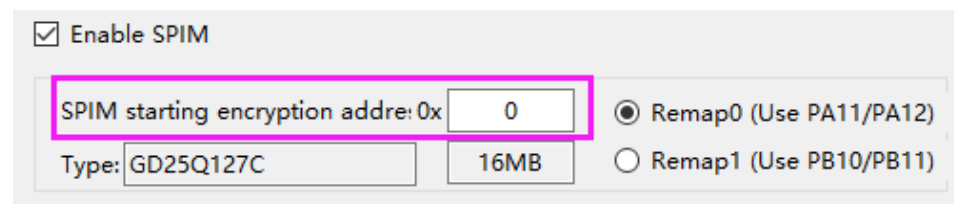
External memory encryption principle:

When the external memory encryption download is required, the encryption range and encryption key of the external memory require to be configured first (set the Key in the user system data), then proceed with the download operation. At this time, the MCU will use its internal setting algorithm to encrypt the downloaded original data according to the encryption range and encryption key, and then write the encrypted data to the external memory.

When the encrypted data from the external memory is required to be read, it also requires to configure the encryption range and encryption key that set during encryption. The MCU will decrypt the encrypted data according to its internal setting algorithm, using the encryption range and encryption key to restore the correct original data.

When downloading file from external memory, this tool can be set to encrypt the download content through the following steps.

Step 1: Set the external memory encryption range, as shown below:



☒ Enable SPIM

SPIM starting encryption address: 0x ☒ Remap0 (Use PA11/PA12)

Type: ☐ Remap1 (Use PB10/PB11)

The encryption range can be set, starting from 0x08400000. If the encryption is not required, set it to 0.

Step 2: Set the external memory encryption Key. Using the “User System Data” page to set, as shown below:

Access protection

FAP:

Disable

SRAM

EOPB0:

System setting byte

SSB:

☒ nWDT_ATO_EN

☒ nDEPSLP_RST

☒ nSTDBY_RST

☒ BTOPT

Erase and program protection bytes

Name	Start address	End address	Size	EPP	
<input type="checkbox"/> Sector0	0x8000000	0x80007FF	0x800(2K)	N	<div>EPP0: <input type="text" value="FF"/></div> <div>EPP1: <input type="text" value="FF"/></div> <div>EPP2: <input type="text" value="FF"/></div> <div>EPP3: <input type="text" value="FF"/></div> <div><input type="checkbox"/> Select all</div>
<input type="checkbox"/> Sector1	0x8000800	0x8000FFF	0x800(2K)	N	
<input type="checkbox"/> Sector2	0x8001000	0x80017FF	0x800(2K)	N	
<input type="checkbox"/> Sector3	0x8001800	0x8001FFF	0x800(2K)	N	
<input type="checkbox"/> Sector4	0x8002000	0x80027FF	0x800(2K)	N	
<input type="checkbox"/> Sector5	0x8002800	0x8002FFF	0x800(2K)	N	

User data

Date	0	1	2	3	4	5	6	7
Data 0---7 (0x)	FF	FF	FF	FF	FF	FF	FF	FF

Clear

Load...

Save...

SPIM encryption key

KEY0: 0x

KEY1: 0x

KEY2: 0x

KEY3: 0x

KEY4: 0x

KEY5: 0x

KEY6: 0x

KEY7: 0x

Load from device

Apply to device

Load from file

Save to file

This is the encryption/decryption key for downloading and reading data within the encrypted range of external memory. When the access protection is released, the Key will also be erased.

Step 3: The encryption download can be achieved by downloading file to the external memory as normal.

Copyright© 2023 by HOLTEK SEMICONDUCTOR INC. All Rights Reserved.

The information provided in this document has been produced with reasonable care and attention before publication, however, HOLTEK does not guarantee that the information is completely accurate. The information contained in this publication is provided for reference only and may be superseded by updates. HOLTEK disclaims any expressed, implied or statutory warranties, including but not limited to suitability for commercialization, satisfactory quality, specifications, characteristics, functions, fitness for a particular purpose, and non-infringement of any third-party's rights. HOLTEK disclaims all liability arising from the information and its application. In addition, HOLTEK does not recommend the use of HOLTEK's products where there is a risk of personal hazard due to malfunction or other reasons. HOLTEK hereby declares that it does not authorise the use of these products in life-saving, life-sustaining or safety critical components. Any use of HOLTEK's products in life-saving/sustaining or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold HOLTEK harmless from any damages, claims, suits, or expenses resulting from such use. The information provided in this document, including but not limited to the content, data, examples, materials, graphs, and trademarks, is the intellectual property of HOLTEK (and its licensors, where applicable) and is protected by copyright law and other intellectual property laws. No license, express or implied, to any intellectual property right, is granted by HOLTEK herein. HOLTEK reserves the right to revise the information described in the document at any time without prior notice. For the latest information, please contact us.