NuMicro[®] Cortex[®]-M Code Protection

Application Note for 32-bit NuMicro[®] Family

Document Information

Abstract	This document is aimed to introduce many kinds of ways provided by Nuvoton to protect code or data from being pirated.
	Meanwhile, the ICP, ISP and NuGang Programming tools and software programming sequences that can help users to utilize in the system or in mass production are described in this document.
Apply to	NuMicro [®] Cortex [®] -M0/M4 Series

The information described in this document is the exclusive intellectual property of Nuvoton Technology Corporation and shall not be reproduced without permission from Nuvoton.

Nuvoton is providing this document only for reference purposes of NuMicro microcontroller based system design. Nuvoton assumes no responsibility for errors or omissions.

All data and specifications are subject to change without notice.

For additional information or questions, please contact: Nuvoton Technology Corporation.

www.nuvoton.com

Table of Contents

1	OVERVIEW
2	SECURITY LOCK4
	2.1 Associated Registers 4
3	CODE PROTECTION BY NUVOTON TOOLS5
	3.1 Enable Security Lock via ICP or ISP Tool5
	3.2 Code Protection in ICP Offline Mode
4	UID & UCID SECURITY PROTECTION9
	4.1 What is UID?
	4.1 What is UID?
	4.1 What is UID? 9 4.2 UID Security Protection 9 4.3 What is UCID? 10
	4.1 What is UID?94.2 UID Security Protection94.3 What is UCID?104.4 UCID Security Protection10
	4.1 What is UID?94.2 UID Security Protection94.3 What is UCID?104.4 UCID Security Protection104.5 How to Read UID & UCID?12
5	4.1 What is UID?94.2 UID Security Protection94.3 What is UCID?104.4 UCID Security Protection104.5 How to Read UID & UCID?12SPARE REGISTER IN RTC13
5	4.1 What is UID? 9 4.2 UID Security Protection 9 4.3 What is UCID? 10 4.4 UCID Security Protection 10 4.5 How to Read UID & UCID? 12 SPARE REGISTER IN RTC 13 5.1 Tamper Pin

1 Overview

Nowadays microcontrollers (MCUs) can be seen anywhere as they are flexible, robustness and easy to develop. Users always consider "code or data security" an important factor while the MCU is implemented in the system.

In view of code protection, there is an easy way to force flash inside the MCU to be locked after mass production. However, some applications need advanced functions in case someone tries to break the chassis to steal the important data therein.

Nuvoton considered "code or data security" in the very early stage of design. To protect the flash in NuMicro[®] Cortex[®]-M0/M4 series, the security lock bit in "User Configuration" is a simple but powerful way to lock the chip data after mass production.

User can update the MCU program memory under software control by Nuvoton ICP programming tool without removing the mounted MCU chip from a target PCB. The ICP tool provides a very friendly way to all the flash programming settings, including User Configuration.

Nuvoton also provides a particular register, spare register, and a corresponded pin, Tamper pin, for customers who have specific key or data to protect. While the voltage change happened on the Tamper pin, the data in the spare register will be automatically cleared.

In addition, Nuvoton provides special mechanism, UCID (Unique Customer Identification), to strengthen code protection. Users could add this special and customized ID into source code to strengthen the barrier of stealing code by others. Meanwhile, no one else but customer signed the non-disclosure agreement (NDA) could purchase the chip with same UCID.

In summary, this document is aimed to introduce five ways to protect the code or data from being pirated for NuMicro[®] Cortex[®]-M0/M4 series. Users could easily implement these mechanisms in each system and select a suitable way based on different applications.

- Security lock in Config0 register
- Code protection by Nuvoton tools
- 96-bit Unique Identification (UID)
- 128-bit Unique Customer Identification (UCID)
- RTC spare register and Tamper / Snooper pin

2 Security Lock

The protection mechanism can prevent the original source code from being stolen. In addition, Nuvoton provides other applications to enhance and strengthen the protection of user's source code. Please refer to the UID & UCID Security Protection section for details.

2.1 Associated Registers

Nuvoton provides a function for the NuMicro[®]-M0/M4 to lock the chip securely by means of the user configuration register, Config0[1], LOCK bit. As shown in Table 2-1, if the LOCK bit is set as 0, user can only get the chip's data in Config0 and Config1 through Nuvoton's ICP programming tool, NuGang programmer, or a third party programming tool, and the other data in flash will be shown as 0xFFF_FF.

31	30	29	28	27	26	25	24
CWDTEN[2]	CWDTPDEN	Reserved		CGPFMFP	CFOSC		
23	22	21	20	19	18	17	16
CBODEN	CBODEN CBOV			Reserved			
15	14	13	12	11	10	9	8
		Reserved			CIOINI	Rese	erved
7	6	5	4	3	2	1	0
CI	BS	Reserved	CWDT	E[1:0]	DFVSEN	LOCK	DFEN

Config0 (Address = $0x0030_0000$)

		Security Lock
		0 = Flash data is locked.
		1 = Flash data is not locked.
[1]	LOCK	When flash data is locked, only device ID, CONFIG0 and CONFIG1 can be read by writer and ICP through serial debug interface. Others data is locked as 0xFFFFFFFF. ISP can read data anywhere regardless of LOCK bit value.
		User need to erase whole chip by ICP/Writer tool or erase user configuration by ISP to unlock.

Table 2-1 LOCK Bit in Config0 Register

3 Code Protection by Nuvoton Tools

3.1 Enable Security Lock via ICP or ISP Tool

Besides the third party writer, user can also use Nuvoton's NuMicro ICP or ISP Programming Tool to lock the source code during the process of chip programming. Moreover, Nuvoton provides an interface for user to get the contents of flash data from the On-board Flash window wherein the flash data is changed to 0xFFFF_FFFF after the ICP tool finishes "Security Lock" process. Through such a convenient tool, source code protection can be greatly improved. If someone wants to read the flash data of the locked chip, the ICP tool will pop out a warning window to enforce the whole chip erase. Figure 3-1 shows the flow of how to set the chip locked.

	Step 1 Connect the target chip with Nuvoton
Project Chips Tool Language	ICD Programming Tool
ΠυνοΤοη	ICP Programming 1001.
status Step 1.	Step 2. Click "On-board Flash" button and the
Disconnect Chip Connected with Nu-Link (ID: 7788ca99)	data will be shown below.
Part No. NUC140VE3CN LDROM:4K, APROM:128K, Data:0K, RAM:16K	Stop 2 Click "Sotting" button for ship options
007000	Step 5. Click Setting button for chip options
Load me	Step 4. Select "Security Lock" to lock the chip
size 3960 Butes cherksum effed	when ICP finishing programming.
ADDOM File name: C:\Nuvolon\RSP1ibran\NUC100SeriesRSP.v1.05.002\NuvolonPlatform Keil\	
size 5864 Rules check um dhab	Chip Options
Data Elash File name CMIsers/IBDI/Deskton/Firmware/MI/C1xx I/F M0 cks hin	Clock source selection
	External crystal clock (4**24MHz)
Step 3. Configurations bits	Internal RC 22MHz oscillator clock
Setting Config 0: 0xFFFFFFF Config 1: 0x0001FE00 - Select -	Brown out voltage
File data Stop 2 Onboard Flash Offine Flash	● 4.5v ○ 3.8v ○ 2.7v ○ 2.2v
LDROM APROM Data Flash LDROM APROM Data Flash LDROM APROM Data Flash Info	Boot select
000000000: 00 06 00 20 69 01 00 00 89 01 00 00 88 01 00 00 A	O LDROM @ APROM
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 0	Step 4.
00000040: A9 03 00 00 A3 01 00 00 E5 05 00 00 09 06 00 00 00000050: 2D 06 00 00 6D 06 00 00 A3 01 00 00 A3 01 00 00 32 bits	Brown Dut Reset Enable
00000060: ED 0C 00 00 A3 01 00 00 A3 01 00 00 A3 01 00 00 A5 01 00 00 000000070: E1 0D 00 00 1D 0E 00 00 F9 08 00 00 5D 09 00 00 000000080: C1 09 00 00 25 0A 00 00 A3 01 00 00 5D 09 00 00	Data Flash Enable
000000000: A3 01 00 00 SaveAs	Data Flash Base Address: Ox 1FE00
00000080: D1 08 00 00 A3 01 00 00 A3 01 00 00 A3 01 00 00 000000000 00 E0 02 E8 00 E0 40 E8 00 A0 30 C8 08 38 24 18 Refresh	Conformation
Program	Conlig 0: 0xFFFFFFFD Conlig 1: 0x0001FE00
LDROM APROM Data Flash Config Option Start	
Build 5320rc	Cancel
Nuvoton NuMicro ICP Programming Tool 1.18 - NUC100 series	Step 5 When ICP finished programming the data, the flash
Project Chips Tool Language	Step 5. When fer finished programming the data, the flash
ΠυνοΤοη	miorination window will be not capable of reading.
Status	Step 6. Click the "Yes" button to erase the whole chip
Disconnect Chip Connected with Nu-Link (ID: 7788ca89)	Step 7. Chip's data is completely erased.
Part No. NUC140VE3CN	Navorton Nubliam ICR Programming Tool 118 x NIC100 series
Load file	Project Chips Iool Language
LDROM NuMicro ICP Programming Tool	ηυνοΤοη
	Status Disconnect Dis Connected with NuLink (D: 7780ca89)
APROM Flash lock protected! IuvotonPlatform_KeiK	Part No. NUC140VE2CN LDR0M-8K, APR0M-128K, Data 0K, RAM-16K. UID ALCO:
Press "Yes" to try to erase the whole chip,	Load Re
Press "Yes" to try to erase the whole chip, "No" to try to connect again, "Cancel" to disconect.	Lood IIe L000M File name CVRogram FileNouston Tosh/CPTo0Ne_Link/XCZ_SP3en
Press "Yet" for ty to ensue the whole chip, "No" to try to conset again, "Cancel" to disconect. Step 6.	Land Ite LDRDM. File name C:Ofing ann File Whardoon Toolf VOPT on Mile Link VCE_JSP bin inter 3550 Bytes, checkharm elbel Aproport File name C:Windowshill States WHATCHOSene359 / 10.5022 WandowsPatteres Yaff.
Press Yes' to ty to ense the whole chip, No to try to conset again, "Cancel" to disconcet. Step 6. Yes No Cancel	Las/Ib LDDOM Firemann: CVIngen/Fe/Nummer/Lob/ICF od/Nu_Las/ICE_JSP2en doi: 3560 Bytes: declaran effed APSCN: Firemann: CVInsected/BSP Learnes/HU/LCIOSeedSF9_v10.5022NuestorPatem_Las/I are 9549 Hump: declaram 4040
Press Test for ty to ensue the whole chip, No to try to consult again, "Cancel" to disconcet. Step 6. Setting	Lad Ib LIDON Flemans C-Ungen Fledbaum fledbaum foldtOF od Nu, Leis VOL JSP ben se: SXR Byer, deckam filed ARBOM Flemans C- VSuederBSP Leader Strategies (SSDD NuederPlatem Jr.aN) se: SXR Byer, deckam Au DearFlaub Flemans C-VSued LEOV Deckap FirmmerVVCT m, EL, M, dis Jan
Press Test for ty to ense the whole chip, No to try to conset again, "Cancel" to disconect. Step 6. Yes No Cancel File data Step 5. On-boad Rash Office Flash	Lad lie LINOX File name: C-Vingan FlexNovien Tools/CPT od/Nu_Link/CC_JSP.bn ce::::500 File name: C-Vin-vori/SP-David/VIC/COS-ee85P_v10.5002NovievPlates_KaN are:::564 File name: C-Vin-vori/SISD-David/Plates_KaN Data File h. File name: C-Vin-vori/SISD-David/Plates_KAN Data File h. File name: C-Vin-vori/SISD-David/Plates_KAN Configurations Ma
Pres Yer to ty to create the whole chip, Not to try to create the whole chip, Not to try to concert again, Concell of disconcet. Step 6. Xes No Cancel • Fielda Step 5. On-boad Fash Office Fash LDROM APROM Data Flash Info	Lad lie LDD: File name: C.19togan File/Munitor Tool/UCP ot/Mu, Lak/UCL_(SP.Ein te: 500 File, deckam rikel AM90M File name: C.19togan File/Munitor File te: 546 File, deckam Rike DataFileh. File name: C.19togan File/Munitor Rikel Carfogan/too Min File name: C.19togan File/Munitor Rike Carfogan/too Min File name: C.19togan File/Munitor Rike File name: C.19togan File/Munitor Rike Carfogan/too Min Same: C.29togan File/Munitor Rike Same: C.29togan Fi
Pres Yer to ty to erase the whole chip, Not to try to conset the whole chip, Cancel to try to conset again, Cancel addisconect. Step 6. Yes No Cancel Fie dals Step 5. On-board Flash Office Flash LOROM LAPROM Data Flash LOROM APROM Data Flash Flash Flash Prom Prom Prom Prom Prom Prom Prom Prom	Las/Ib LDDM Firemen: CVIspan Fire/Naveron Fod/OFF od/NavLas/LLS/SEL in: 256 Diple:, checkan eller APROX Firemen: CVIser/ADV/LDCDE/end/SF_v10.5022/NavdorPatem_Fad/ end/SEL Destable/Firement CVIser/ADV/LDCDE/end/SF_v10.5022/NavdorPatem_Fad/ Destable/Firement/NCL/su/LEL/EL_id.eller Firement Sector Stop 7 Fire das
Press Test for ty to erase the whole chip, Not to try to conset the whole chip, Cancel to disconcet. Seting File data Step 5. On-board Flash DROM APROM Data Flash LDROM APROM DATA Flash F	Las/lb LBDBM File name: CVM-open File/Mourden Todd/OFF od/File.LBX/DC_SP2.en in: 2660 Jpm; disclosure field AR92M File name: CVM-orde/ISP Lase/MCL/06/Ees45P, v16.5022/Norde/File/m_TodV are 954 Mpm; disclosure Adu DearTouch File name: CVM-orde/ISP Lase/File/Adu Configurations Min Service CVM-orde/ISP Lase/File/Adu/SP2 (Service - File das ConfigUrations Min) Service CVM-orde/ISP Lase/File/Adu/SP2 (Service - File das ConfigUrations Min) ConfigUrations Min Offen File Todoward Min Min Min Min Min Min File Todoward Min
Press 'Yes' to ty to create the whole chip, "Created sayin, "Cancel" descenet. Setting File data Step 5. On-board Planh LDROM APROM Data Flanh LDROM APROM Data Flanh Islo @ 8 bin 16 bin 16 bin 16 bin 16 bin 17 bin 18 bi	Lad lie Lindow Pierraem: CVihogam Flerkhousen fods/CPF od/Ne, Liek/CC_SP2er es: 260 Byer, deckam field AR90H Pierraem: CVihor/AB0U Docking/Pierraem/AUC100_EE_MU, do.t.bin Pierra bad Configurations bits Series Config. Config. Jamon AUC100_EE_MU, do.t.bin Pierra bad Configurations bits Series Config. Jamon AUC100_EE_MU, do.t.bin Diffee Flanh Lindow Ladfreid Configuration AUC100_EE_MU, do.t.bin Pierra Bad
Pres Yer to ty to create the whole chip, We to try to concert again, Concert od accenet. Step 6. Yes No Cancel Fie data Step 5. On-board Flash Office Flash LDROM APROM Data Flash LDROM APROM Data Flash Info @ 8 bits @ 8 bits @ 32 bits @ 32 bits	Las/Ib LDDM Fir name: CVIngen Fin/Navren CabloP ColfseLLasVCL_SP2n ar: 3560 Pytes, cleation, elled AFBOR: Fir name: CVInn/SEU/CasloBCF, v1.6.5022NuotorPatem_LasVC ar: 3564 Pytes, cleation, elled Data Fahn, Fir name: CVInn/SEU/CasloBCF, v1.6.5022NuotorPatem_LasVC Data Fahn, Fir name: CVInn/SEU/CasloBCF, v1.6.5022NuotorPatem_LasVC Data Fahn, Fir name: CVInn/SEU/CasloBCF, v1.6.5022NuotorPatem_LasVC Data Fahn, Fir name: CVInn/SEU/CasloBCF, v1.6.5000 Congo garranger provide family filter Fahn, filter Fa
Pres Ver To ty to erase the whole chip, "Craned" to attract again, "Craned" to attract again, "Craned" to attract again, "Craned" to attract again, "Craned" attract a	Las/Ib L000M Fin rame: CVIugen Fin/Vhurten Todi/CFT od/Hu_Lai/CL_SCL_SF2an de: 260 Byte: checkan she ARDON Fin rame: CVIugen/Set/Vhurten/Todi/Set/Set/Set/Set/Set/Set/Set/Set/Set/Set
Pres Yer To ty to create the whole chip, "Cancel" to try to create tagain, "Cancel" to disconcet. Step 6, Yes No Cancel Fie das Step 5. On-boad Flash DROM APROM Data Flash LDROM APROM Data Flash Info BROM APROM Data Flash LDROM APROM Data Flash Info B bit 16 bits Save As Refereth	Lastle Lastle LBDBH Pie name CVBugen Findhussen fodd/07 fod/Hg_Lisk/CC_SP2in ein: 2600 Bjert, deckan field ARQM Pie name CVBuc/00109 Bage MULCID/Sealey 7, 15.5020 Musc/Pietim_Tail/ ein: 954 Big., deckan field Dearthanh Pie name CVBuc/UD07 Deatage/Finneer/MUCIeu/CE_MB_ds.les Configurations Big. Configurati
Pros Yes' to ty to create the whole chip, We to try to create the whole chip, We try to concert again, Concert adacement. Setting Field das EDROM APROM Data Flash LOROM APROM Data Flash Into Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Program Pro	Lad la Lad lad la Lad lad lad lad lad lad lad lad lad lad l
Pres Yer To ty to create the whole chip, "Created again," Concell of disconect. Step 6. Yee No Cancel Fie data Step 5. On-board Flash Office Flash CROM APROM Data Flash DROM APROM Data Flash Info Program Program Program Program Program Cannot execute reading process through ICP tool	Lasfie Loop Parameter CV-togen Face/Nuclear Code/OF 00/Hau_LasVCL_ISF2e ext 2500 Parameter CV-togen Face/Nuclear Code/OF 00/Hau_LasVCL_ISF2e ext 2500 Parameter CV-togen Face/Nuclear Code/OF 00/Hau_LasVCL_ISF2e ext 2500 Parameter CV-togen Face/Nuclear CV-togen
Press Yer To ty to create the whole chip, "Created again," "Created again," "Crea	Los file Los fi

Figure 3-1 "Security Lock" Flow in the ICP Tool

3.2 Code Protection in ICP Offline Mode

Except enabling the **Security Lock** option to set the chip locked for source code protection as described in the previous section, Nuvoton provides another chip protection mechanism in Offline mode with the ICP tool.

When using Nuvoton's "Nu-Link" or "Nu-Link Pro" programming tools (as shown in Figure 3-2) to program a chip in Offline mode, there are two methods to protect chips - "setting password for offline data" or "limiting the number of offline programming". Figure 3-3 shows the steps of setting the password or the maximum number of programming in Offline mode.



Figure 3-2 Nu-Link and Nu-Link Pro Programming Tool

Nuvoton NuMicro ICP Programming Tool 1.18 - NUC100 series Project Chips Tool Language	Program Option
Status Step 1. Connect the target chip.	Uperation ♥ Erase ♥ Program ♥ Verify Step 3.
Load Re LOROM File name: C:\Program Files\Nuvoton Tools\ICPTool\Nu_Link\ICE_ISP.bin	Write software serial number Select "Offline programming □ Reset chip after programming mode " for offline setting.
size: 3960 Bytes, checksum: e3ed APROM File name: C:\Nuvoton/BSP Lbray\NUC100SeriesBSP_v1.05.002\NuvotonPlatform_Kel\{ size: 5964 Bytes, checksum: 4bab	Software serial number (SN) Increase SN from Dx 180000004
Data Flash File name: C:\Users\LBDU\Desktop\Firmware\NUC1xx_UCE_M0_ck:x bin File not load Configurations bits	Step 4. Enter the password to protect Options for offline programming mode Enter the password to protect
Setting Config 0: 0xFFFFFF Config 1: 0x0001FE00 -Select -	Enter password
LDROM APROM Data Flash LDROM APROM Data Flash LDROM APROM Data Flash Info 000000000: 00 80 00 20 45 01 00 00 88 01 00 00 88 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 48 01 00 00 40 00 00 00 00 00 00 00 00 00 00	Repeat password
IO00000501 ED CO OA A3 OA A3 OA A3 OA A3 OA OA	Enter the Max Number to limit the number of offline programming NucLink-Pro ID Voltage number of offline programming Power control is used on NucLink-Pro, and is vasue only a ranger
Program Step 2.	○ 1.8V ○ 2.5V ○ 3.3V ◎ 5.0V
Click the "Option" button for Program Option	Default DK Cancel

Figure 3-3 ICP Offline Mode

For Step 4 in Figure 3-3, user can set any form of password and re-enter the password again to confirm the setting, and then click the Start button to execute the chip programming

process. When the ICP tool detects the chip is connected next time, a request form will appear to ask the user to enter the right password to unlock the chip. If the entered password does not match the preset password, the request window will not disappear until the right one is entered. If user wants to remove the "Password" setting, just enter the right password and undo the click in Step 4 or erase the whole chip data could achieve.



Figure 3-4 Password Function in ICP Tool Offline Mode

Another offline protection mechanism is to limit the number of programming chip when using the "Nu-Link" or "Nu-Link Pro" programming tools to program a chip. When the number of chip programming meets the limitation number, the "Nu-Link" or "Nu-Link Pro" will not be allowed to program any other chips. User needs to erase and re-program "Nu-Link" or "Nu-Link Pro" to continue chip programming again. User can get the flash data in "Nu-Link" or "Nu-Link Pro" from the Offline Flash window as shown in Figure 3-5.

Nuvoton NuMicro ICP Progr	amming Tool 1.18 - NUC100 series							
<u>P</u> roject <u>C</u> hips <u>T</u> ool <u>L</u> angu	age							
ηυνοτοη								
Status Stop check Nu-Link con	nected (ID: 7788a544) Step 6-(2).							
i arrio.								
Load file								
LDROM File name:	C:\Program Files\Nuvoton Tools\ICPTool\Nu_Link\ICE_ISP.bin							
	size: 3960 Bytes, checksum: e9ed							
APROM File name:	C:\Nuvoton\BSP Library\NUC100SeriesBSP_v1.05.002\NuvotonPlatform_Keil\{							
	size: 5864 Bytes, checksum: 4bab							
Data Flash File name:	C:\Users\LBDU\Desktop\Firmware\NUC1xx_ICE_M0_cks.bin							
	File not load.							
Configurations bits								
Setting Config 0:	0xFFFFFFD Config 1: 0x0001FE00 - Select -							
File data	On-board Flash Offline Flash							
LDROM APROM Data Flash	LDROM APROM Data Flash LDROM APROM Data Flash Info							
Offline programming data create	d on Fri Mar 23 20:07:34 2012							
* Target chip type: NUC100 seri * Do not reset chip after program	es ming							
* Limit the programming number: * Do not use auto-programming	10							
* Nu-Link-Pro IO voltage: 5000m * Statistics								
Programming totally 4 times Programming failed 2 times	Programming totally 4 times Programming failed 2 times							
Program								
LDROM APROM	Data Flash Config Dption Start							
	Build: 5320rc							

Figure 3-5 Offline Flash Data in the ICP Tool

Both setting the password or limiting the maximum number of chip programming in Offline mode provide further protection for chip programming.

4 UID & UCID Security Protection

4.1 What is UID?

UID (Unique Identification) stands for a specific code for every chip dispatched from Nuvoton, just like an identification card which is unique for everyone. UID represents chip's part number and date of dispatching with length of 96 bits.

Why UID is so special for the chip's encryption issue? User may worry or concern about if any industrial agent or person with intensions steals the source code when a commodity is under development or developed stage. Then, the person may try to get the same IC to achieve the same function as user designed. Therefore, Nuvoton provides a unique ID for every NuMicro[®]-M0/M4 chip so that user could employ UID into source code. The UID protection mechanism will be introduced in the next section.

4.2 UID Security Protection

To enhance the degree of safety for user's source code, each NuMicro[®]-M0/M4 chip dispatched from Nuvoton will be planted with a unique ID in the chip. User can put UID, which is dealt with DES (Data Encryption Standard), into Data Flash or some specified area. Also, users can design the standard of encryption by themselves to protect the source code in the chip from being stolen and produced by other people with specific intensions.

Figure 4-1 shows the flow that UID needs to be dealt with DES and put into Data Flash. Then user can add a judging method in the firmware code to compare the current chip's UID with the previous one. If the result is not the same, the program will fall into dead loop. Consequently, it will greatly prevent user' commodity to be mass produced from source code being stolen, under this double protection mechanism from UID (Nuvoton) and DES (user). Moreover it also significantly increases user's confidence and reliability to use Nuvoton IC.



Figure 4-1 UID Protection Flow

4.3 What is UCID?

UCID (Unique Customer ID) is an initiative technique provided by Nuvoton to protect chip's source code. In addition to the previous UID section, user can apply for customized UCID with Nuvoton to ensure chip safety.

4.4 UCID Security Protection

Firstly, user provides the product number or specific code to put into the UCID. User data will be encoded and the conversion result will be planted into the chip to become customized and highly protected. Figure 4-2 shows the flow about how UCID protects the chip's source code, and Figure 4-3 shows the information to be put into the UCID.



Figure 4-2 UCID Protection Flow



Figure 4-3 UCID Information

User can connect to a chip through Nuvoton's "NuMicro ICP or ISP Programming Tool" to get the current UCID in the chip as shown in Figure 4-4.

Status Disconnect	Chip Connec	ed with Nu-Link (ID: 7	78 a54 UCID:5	tion of targe 4K, APROM: 00000-2A22 5413933-FF4	et chip, 64K, Data:4K, RAM:4K 10782-A6050000 183535-FFFFFFFFFFFFFFFFFFFFF		Step 1. Connect chip with Nuvoton ICP tool Step 2. Click the "Connect" button
Part No.	M0516LBN	LDROM:4K, AF UID/UCID:	PE 1:6419 / 2021-91	, n.8.₩. 4N		1	Step 3. Move the cursor on the right of part NO. Step 4. The information of target chip will be shown
Load file		CH DROM have					
LDROM	rile name:	C. LDH OM: Nex					
		File not load.					Zoom In
APROM	File name:	C:\APROM.hex					<u>× </u>
		File not load.				r	
Data Flash	File name:	C:\Data.hex					Information of target chip,
		File not load.					
Configurations b	its						IDROM-4K APROM-64K Data-4K RAM-4K
Setting	Config 0:	0xFFFFFFFF		- Sele	ct · 🗸 👻		UID-E100000-20220782-06050000
File data		On-board Flash	Off	ine Flash			UCID-E6412022 EE4E2E2E EEEEEEE EEEEEEE
LDBOM APR	OM Data Flash	LDBOM APROM	Data Flash LDF		Data Flash Info		0010,30413333-11403535-111111111111111111
00000000: 0000010: 00000030: 00000040: 00000060: 00000060: 00000080: 00000080: 00000080: 00000080:	. . 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 03 00 00 49 01 00 00 49 01 00 00 49 01 00 00 81 07 00 00	69 01 00 00 8F 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 91 00 00 00 00 00 01 00 00 00 A3 01 00 00 A7 06 00 00 A9 01 00 00 A9	01 00 00 00 00 00 01 00 00 06 00 00 01 00 00			7
Program							
LDROM	🔽 APROM	📃 Data Flash	🔽 Config	Option	Start		

Figure 4-4 UID and UCID Data via ICP Tool

As to the protection mechanism for UCID, user can add a judging method in the firmware code to compare the current chip's UCID with the one encoded by Nuvoton. If the result is not the same, the program will fall into dead loop. Even user connects the chip with the ICP tool, an error window will appear to enforce the whole chip erase. According to this particular protection mechanism, the possibility of source code being stolen will be decreased, and product competition will be enhanced.

The NuMicro[®]-M0/M4 series chips from Nuvoton are normally dispatched without UCID and top-printed on chips. If user wants to add this protection mechanism to the purchased chips, please contact <u>numicro@nuvoton.com</u> for further information.

4.5 How to Read UID & UCID?

Before reading UID or UCID, user needs to unlock a register to get the access to control the flash related register first and then enable ISP functions.

```
SYS_UnlockReg();
void FMC_Open(void)
{
    FMC->ISPCON |= FMC_ISPCON_ISPEN_Msk;
}
```

The following illustrates the programming sequences about how to read UID & UCID back via FMC related commands.

```
//This function reads one of the three UID.
uint32_t FMC_ReadUID(uint32_t u32Index)
{
    FMC->ISPCMD = FMC_ISPCMD_READ_UID;
    FMC->ISPADR = 0x04 * u32Index; //u32Index must be 0, 1, or 2.
    FMC->ISPTRG = FMC_ISPTRG_ISPGO_Msk;
    while (FMC->ISPTRG & FMC_ISPTRG_ISPGO_Msk) ;
    return FMC->ISPDAT;
}
```

Table 4-1 Macro of Reading UID

```
//This function reads one of the three UID.
uint32_t FMC_ReadUCID(uint32_t u32Index)
{
    FMC->ISPCMD = FMC_ISPCMD_READ_UID;
    FMC->ISPADR = (0x04 * u32Index) + 0x10; //u32Index must be 0, 1, 2 or 3.
    FMC->ISPTRG = FMC_ISPTRG_ISPG0_Msk;
    while (FMC->ISPTRG & FMC_ISPTRG_ISPG0_Msk) ;
    return FMC->ISPDAT;
```

Table 4-2 Macro of Reading UCID

5 Spare Register in RTC

Some applications need to protect certain critical data like electronic safety deposit box or specific ID cards. User can utilize a special pin to detect any voltage change happened on this pin. If someone wants to tamper the data inside, the chip will activate the protection mechanism.

Some NuMicro[®] Cortex[®]-M0/M4 series, such as NUC100, NUC200/220AN, NUC230/240AE, Nano100AN, Nano100BN, Nano102/112, NUC442/472, M451 and NUC505 series, are embedded with RTC peripheral. Also, some of them are provided with a special register to store important information. The spare register content is cleared when specified event on tamper pin is detected.

This special function related to data protection is "Spare Register". The following table lists all the NuMicro[®] Cortex[®]-M series which support spare register function or not.

NuMicro®	RTC	Spara Eurotion	Spare Reg.
Cortex [®] -M	Function	Spare Function	Length
NUC505	\checkmark	\checkmark	32 bytes
NUC442/472	\checkmark	\checkmark	96 bytes
M451	\checkmark	\checkmark	80 bytes
Nano100	\checkmark	\checkmark	80 bytes
Nano102/112	\checkmark	\checkmark	80 bytes
NUC230/240AE	\checkmark	\checkmark	80 bytes
NUC200/220AN	\checkmark		
NUC100	\checkmark		
NUC122/123			
NUC029			
M058S			
M0518			
M051			
Mini51			

Table 5-1 RTC and Spare Function Support List

5.1 Tamper Pin

Taking M451LG6AE as an example, the RTC is equipped with 80 bytes spare registers to store important user information, and also has a snoop function to detect the transition of snooper pin.

User needs to enable SPRRWEN (RTC_SPRCTL[2]) before writing one of 20 spare registers (RTC_SPR0 ~ RTC_SPR19). User could read SPRRWRDY (RTC_SPRCTL[7]) to check if data has been written into registers or not. User could only access the spare registers again once SPRRWRDY is 1. Any access to spare registers is available if SPRRWRDY is 0.

The snoop detection function is used to detect the transition of TAMPER pin. When the transition condition defined in SNPTYPE1 (RTC_SPRCTL[3]) and SNPTYPE0 (RTC_SPRCTL[1]) is detected then 80 bytes spare registers (RTC_SPR0 ~ RTC_SPR19) content will be cleared by hardware automatically to prevent the security data from being disclosed

NuMicro [®] Cortex [®] -M	Tamper Pin Function	Pin Configuration	
NUC442/472	\checkmark	PA.0/PA.1	
M451	\checkmark	PF.2	
Nano100	\checkmark	PC.13/PB.15	
Nano102/112	\checkmark	PB.8	
NUC230/240AE	Note: Because NUC230/240AE and NUC505 do not have		
NUC505	Tamper pin so that its s for code protection.	pare register could not be used	

Table 5-2 Tamper Pin in Each Series

5.2 RTC Spare Register

Table 5-3 shows 20 separated spare registers for storing important information. Each register is 4 bytes long and a total of 80 bytes important data could be stored.

Register Offset		R/W	Description	Reset Value	
RTC_SPR0	RTC_BA+0x40	R/W	RTC Spare Register 0	0×0000_0000	
RTC_SPR1	RTC_BA+0x44	R/W	RTC Spare Register 1	0×0000_0000	
RTC_SPR2	RTC_BA+0x48	R/W	RTC Spare Register 2	0x0000_0000	
RTC_SPR3	RTC_BA+0x4C	R/W	RTC Spare Register 3	0x0000_0000	
RTC_SPR17	RTC_BA+0x84	R/W	RTC Spare Register 17	0×0000_0000	
RTC_SPR18	RTC_BA+0x88	R/W	RTC Spare Register 18	0×0000_0000	

31	30	29	28	27	26	25	24		
SPARE									
23	22	21	20	19	18	17	16		
	SPARE								
15	14	13	12	11	10	9	8		
	SPARE								
7	6	5	4	3	2	1	0		
SPARE									

Bits	Description		
[31:0]	SPARE	Spare Register	
		This field is used to store back-up information defined by user.	
		This field will be cleared by hardware automatically once a snooper pin event is detected.	
		Before storing back-up information in to RTC_SPRx register, user should write 0xA965 to RTC_RWEN[15:0] to make sure register read/write enable bit REWNF (RTC_RWEN[16]) is enabled.	

Table 5-3 RTC Spare Register Table and Description

Revision History

Date	Revision	Description
2015.07.28	1.00	1. Initially issued.

Important Notice

Nuvoton Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, the control or operation of dynamic, brake or safety systems designed for vehicular use, traffic signal instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at customer's risk, and in the event that third parties lay claims to Nuvoton as a result of customer's Insecure Usage, customer shall indemnify the damages and liabilities thus incurred by Nuvoton.

Please note that all data and specifications are subject to change without notice. All the trademarks of products and companies mentioned in this datasheet belong to their respective owners.