501 保密模式下的程序运行

V1.0

Publication Release Date: May. 2009

Table of Contents

1. 前言

NUC501 是以 ARM7TDMI 为核心的 32 位单片微机，提供高达 108MHz 的运作频率，满足高速运算需求的工作。501 除了内建 32 Kbytes SRAM 外，也支持透过 SPI interface，对外部内存(SPI Memory)进行存取，令系统的内存具有高度的扩充性。

然而由于程序记忆放置于芯片外部，因此就有被他人读取的风险，为了达到程序的保密，NUC501 提供了 OTP 编码的功能，这功能可以使得放置在 SPI Memory 上的程序，可以是被加过密的数据，OTP 编码功能一旦启动了之后，如果没有正确的密钥，就只能看到乱码般的数据，藉此保障用户所设计的程序数据。

由于一旦启动 OTP 的保密功能，NUC501 在程序及数据的读取上，都会同没有启动 OTP 前有所不同，本文件将就这些不同来作说明。

2. OTP 简介

2.1. 什么是 OTP

在 NUC501 中，为了要对用户的程序进行加密保护的动作，必须要先由用户提供一个用来加密的金鑰，将这金鑰储存于芯片中，之后并禁止读取或移除这个金鑰。为了达到这个目的，NUC501 内建了一次性可编程内存 One Time Programmable Read Only Memory (OTPROM)，简称 OTP，并只提供 OTP 写入，而无读取功能，以保护 OTP 内部的数据。

2.2. 如何写入 OTP

OTP 的写入需到用到高压的电路，但是 NUC501 在一般工作模式，都是使用 3.3V 以下的电压，因此要对 OTP 进行写入，就需要另外有特殊的硬件配合。因此 Nuvton 为 NUC501 的 OTP 写入提供了 OTP Writer Board 的硬件，同时也提供了相对应的 Windows 工具，将 OTP 的写入简化到只需要几个简单的动作便可完成，详细 OTP Writer Board 操作流程，请参阅 OTP Writer Board User's Manual。

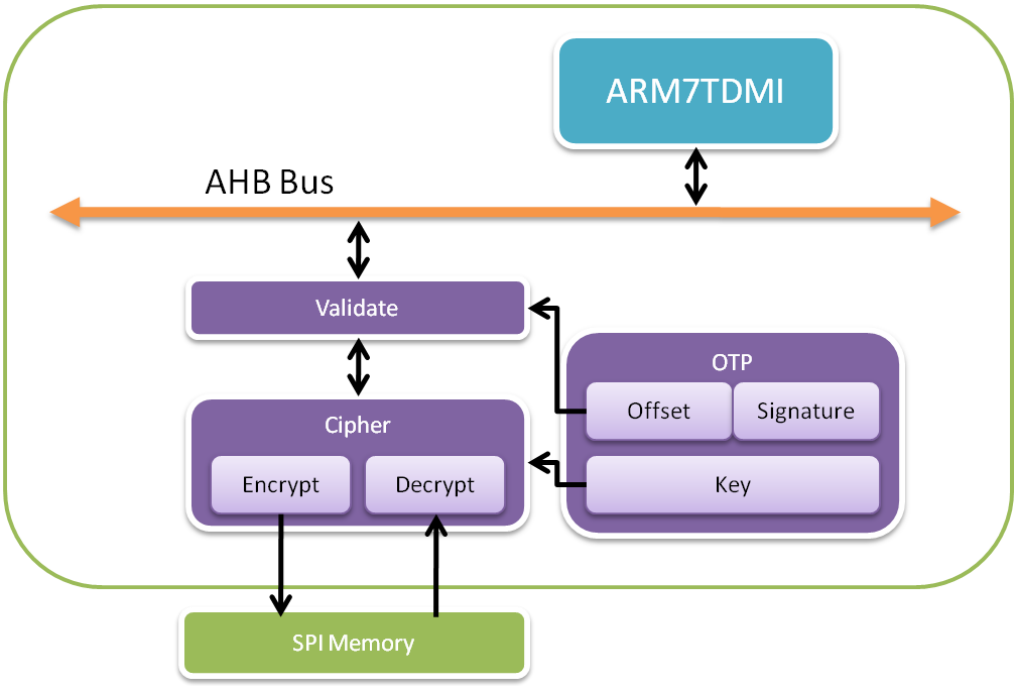
3. NUC501 保密机制

在这节中，我们将说明 OTP 加密功能一旦打开，NUC501 将会有哪些相应的动作，来进行数据的保密。

基本上 NUC501 的加密机制可分为两大部份，一个是建立密钥，一个是建立标识符，建立密钥的目的是为了对用户程序进行加密，而标识符的功能则是确保程序码不被置换成别的代码。

由下图可以看出，所有读写 SPI Memory 的数据，都会先通过加密器(Cipher)，而加密器则依照 OTP 内所储存的密钥(Key)对所有的数据作编译码的动作，这些动作均直接由硬件完成，所以不会有被探知密钥的可能，同时也不会因多了编解碼动作而有存取数据的延迟。

除了加密器与密钥所提供的编译码功能外，下图中也显示了，NUC501 会通过 OTP 内存的标识符(Signature)，对所读取的代码，进行认证的动作，以避免代码有被置换的情况。



3.1. 启动保密机制

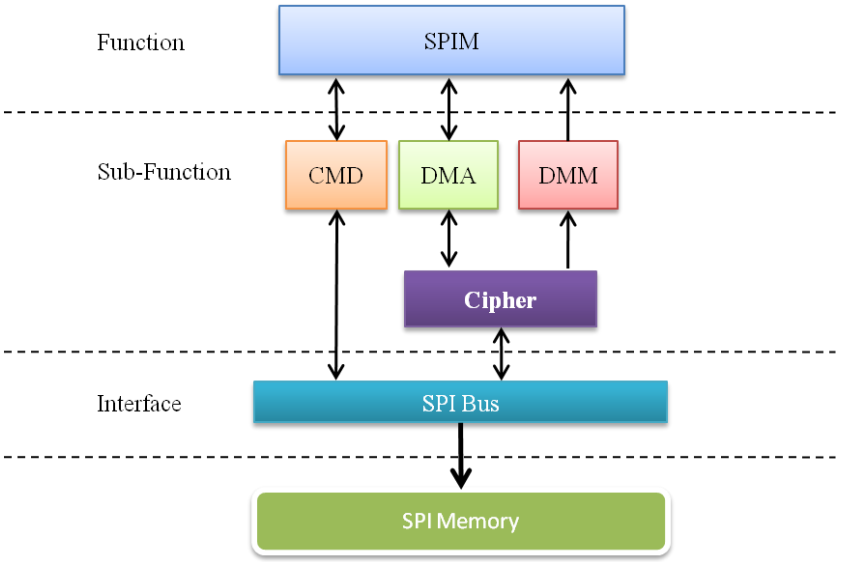
NUC501 的密钥长度为 64-bit，由于它是储存于 OTP 当中，所以本身具有无法读取及移除的特性。一旦建立了密钥，NUC501 的加密器(Cipher)硬件便会启动，所有透过加密器的数据，都会利用密钥来作实时编解碼的动作。而加密器本身存在于 CPU 与 SPI Memory 之间，因此当密钥存在时，NUC501 将自动透过加密器对 SPI Memory 作编解碼的动作。

因此对加密过后的程序而言，如果没有给予正确的密钥，CPU 将无法存取到正确的程序代码及数据，也就无法正常运行了。

3.2. 保密机制下的资料存取

当密钥被写入 OTP 后，NUC501 将会自动启动加密器，之后所有透过加密器的存取，都将进行编码或译码的动作，换句话说，如果不透过加密器对 SPI Memory 作存取，那么数据就不会被编码，也不会被译码，至于存取 SPI Memory 时，是有透过加密器还是没有，则要先了解 SPIM 这个模块的功能。

NUC501 之所以能够由外部的 SPI Memory 开机，便是透过 SPIM 这个模块来完成的，加密器(Cipher)也隶属于这个模块的一部份。SPIM 模块提供了三种 SPI Memory 的存取方式，分别为命令模式(Command mode)，直接内存映像模式(Direct Memory Mapping Mode, DMM mode)，直接内存访问模式(DMA mode)，其中只有命令模式不会透过加密器，其它两种模式都会透过加密器对 SPI Memory 作存取，所以在 OTP 启动的情况下，透过命令模式对 SPI Memory 的读写，将不会被加密或解密，透过其它模式的话，数据就会被编译码。SPIM 的功能架构图如下图所示：



由上图可以看出，SPI Memory 的存取功能是透过 CMD, DMA 及 DMM 三个子功能来完成的，其中 DMA 及 DMM 子功能会先通过加密器(Cipher)才到 SPI Bus 上，而 CMD 子功能则是直接到达 SPI

Bus 上，因此如果有需要在 OTP 启动后，对 SPI Memory 作不加密的数据存取，就必须要透过 SPIM 的命令模式。

3.3. 保密机制下的开机程序

上一节有提到过，当 OTP 启动时，通过加密器的数据，将会利用 OTP 内的密钥进行编译码，同样的，程序的存取也是通过一样的原则。

NUC501 的开机程序，主要有三种模式，分别是 USB Boot, SPI Boot 及 SRAM Boot。其中 USB Boot 主要是为了由 USB 进行 SPI Memory 的刻录动作，SRAM Boot 则是供搭配 ICE 进行程序调试的功能，而 SPI Boot 则可以用来令 NUC501 一开机便直接执行用户的程序。

- USB Boot
  一旦 OTP 被启用，由 USB Boot 模式所写入 SPI Memory 的映像档，也将会是被加密过后的数据，由于同一颗 IC 上，金鑰是相同的，所以理论上由 USB Boot 写入的加密数据，即使不知道密钥是多少，仍应该可以正常被执行，但是因为 OTP 除了密钥的编码外，还会有标识符(Signature)的判断，所以如果无法得知标识符的话，即使利用 USB Boot 模式，把原程序抹除，以新的程序代替，仍无法正常运行，藉此保护程序不会被其它程序取代。

- SRAM Boot
  SRAM Boot 模式，通常是用来进行程序的调试，所以常常会搭配着启用 ICE 模式，而当 ICE 模式启动后，OTP 将会自动关闭，所有对 SPI Memory 的存取将不透过加密器，也不会进行标识符的判断，因此，在 SRAM Boot 模式下，用户虽然可以透过 ICE 或 CPU 去存取 SPI Memory，但也只能看得到 SPI Memory 内被加密过的数据。

- SPI Boot
  SPI Boot 主要是在 NUC501 终端产品所会使用的模式，它会在开机时，将 16KB 的程序数据由 SPI Memory 复制到 SRAM 中，并在 SRAM 中执行它，透过这种方式，来直接运行用户的程序。当 OTP 被启动后，这 16KB 的数据，也将透过加密器的解碼，以确保复制到 SRAM 内的程序是可运行的，当然标识符的验证也会同时进行，如果标识符验证失败的话，复制将不会执行，CPU 也会停止运行。

3.4. 保密机制下的程序更新

如果 NUC501 外接可擦写式的 SPI Memory, ex: SPI Flash, 那么便可以透过将新的程序写入，来进行程序更新的功能，新的程序可以根据用户程序的设计，选择由 UART, SPI, USB 或其它 I/O 接口输入。

如果要进行程序更新的 NUC501，之前已经启动了 OTP 功能，那么就必须要确认写入 SPI Memory 中的更新数据必须是经过相同的密钥加密过的，这部份可在更新时才透过加密器实时编码，也可以给予已用相同密钥编码过的数据，然后不透过加密器，直接写入 SPI Memory。无论是什么样的方式更新，都必须要配合适当的用户程序才能够达成。

除了要确保更新的程序数据是由相同密钥编码过之外，当用户程序将来有更新的需求时，也必须有当初写入 OTP 内的标识符才可以，换句话说，新的程序也要具有相同的标识符才行。

4. Revision History

Version	Date	Description
V1.0	May. 25, 2009	● Created

Important Notice

Nuvoton products are not designed, intended, authorized or warranted for use as components in equipment or systems intended for surgical implantation, atomic energy control instruments, aircraft or spacecraft instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for any other applications intended to support or sustain life. Furthermore, Nuvoton products are not intended for applications whereby failure could result or lead to personal injury, death or severe property or environmental damage.

Nuvoton customers using or selling these products for such applications do so at their own risk and agree to fully indemnify Nuvoton for any damages resulting from their improper use or sales.