Application Report

C2000 器件上的安全启动

Pramod Prabhakara, Karthik Rajakumar, and Christopher Chiarella

摘要

本应用报告讨论了如何使用 TMS320F2838x 器件上的安全闪存启动特性在实际代码执行之前通过附加的启动代码身份验证安全层从闪存执行应用启动。

内容

1 引言 2
2 安全闪存启动概述 2
3 CMAC 身份验证 3
4 安全闪存启动选项 3
5 安全闪存启动流程 4
6 C2000Ware 示例详细信息 5
7 对超过 16KB 的闪存代码进行身份验证 7
8 调试资源 8
9 其他信息和注意事项 8
10 参考文献 8

插图清单

图 3-1. CMAC 工作原理 3
图 6-1. 为 CMAC 启用十六进制实用程序后的 CPU1 示例属性 6

表格清单

表 2-1. 器件上的安全闪存启动概述 2
表 4-1. 安全闪存启动模式配置详细信息 3
表 8-1. 安全闪存启动调试场景 8

商标

1 引言

TMS320F2838x 是一款功能强大的 32 位浮点实时微控制器，专为高级闭环控制应用（如工业电机驱动器、光伏逆变器和数字电源、电动汽车和运输以及感应和信号处理）而设计。该器件支持双核 C28x 架构，并带有可减轻关键通信任务负担的新型连接管理器 (CM)，显著提升了系统性能。虽然这些实时微控制器的硬件效率支持强大的应用，但在创建具体的独特应用程序时使用的是代码。该器件内置的双代码安全模块 (DCSM) 可帮助您创建安全解决方案，而模块中包含的安全启动特性可增强系统能力，以防通过运行您的应用程序来进行未经授权的更新。

DCSM 采用双安全区域概念，因此在闪存一次性可编程 (OTP) 区域中编程的安全配置决定了安全资源（闪存扇区和 RAM）的 Zone1/Zone2/Unsecure 分配情况。除此之外，Zone1/Zone2 资源也可配置为 EXEONLY，从而只允许从该区域执行代码。

更多详细信息，请参阅《*TMS320F2838x 技术参考手册*》[1] 中的 *DCSM* 一章。

2 安全闪存启动概述

与应用程序闪存启动相关的 DCSM 特性之一是能够在执行闪存中的用户应用程序代码之前对其进行身份验证。这样可确保应用程序代码在被编程到闪存存储器后未被篡改，以此确定应用程序代码的完整性。当应用于 Zone1 EXEONLY 闪存扇区时，此特性可用作关键用户应用程序代码的附加安全层。除了传统的闪存启动选项外，安全闪存启动特性还提供了一组额外的启动选项。

安全闪存启动是通过使用 128 位 AES-CMAC 身份验证算法实现的，该算法在会返回通过/失败状态的应用程序代码内容上运行，并且只有在身份验证成功时才继续执行应用程序代码。表 2-1 概述了此特性在器件不同子系统上的情况。每个 CPU 子系统的 BootROM 发起针对该子系统应用代码前 16KB 的身份验证，这称为“主要安全启动”。超出每个 CPU 子系统前 16KB 的应用程序代码的身份验证称为“扩展安全启动”。此过程可由预先进行了身份验证的应用程序代码选择性地发起。

由于在安全闪存启动期间会执行 CMAC 身份验证算法，该启动序列与正常（非安全）闪存启动相比需要更多的时间才能进入用户应用程序。请注意，与 CPU1 或 CPU2 安全闪存启动实现方案相比，器件 CM 内核安全闪存启动需要的时间更少，因为 CM 会使用硬件 AES 加速器。

表 2-1. 器件上的安全闪存启动概述

子系统（内核）	安全启动特性	CMAC 算法实现方案	对闪存启动代码前 16KB 进行身份验证所需的额外时间
CPU1 SS (C28_1)	是	软件（安全 ROM 实用程序）+ AES ROM 表	~400ms（在 INTOSC 上以 10MHz 运行）
CPU2 SS (C28_2)	是	软件（安全 ROM 实用程序）+ AES ROM 表	~20ms（在 PLL 上以 200MHz 运行）
CMSS (CM4)	是	软件（安全 ROM 实用程序）+ 硬件 AES 加速器	~6ms（在 PLL 上以 125MHz 运行）

3 CMAC 身份验证

基于密码的消息身份验证代码 (CMAC) 是一种基于 AES 的身份验证算法，它根据输入数据块构造一种身份验证标签。每次会以 128 位将输入数据块与 128 位 CMAC 密钥一起馈入到加密引擎/软件（根据 CPU 子系统而定）中。该密钥位于 CPU1 USER OTP 的 0x78018-0x7801F 位置，并由器件所有内核上的 CMAC 身份验证算法使用。加密引擎/软件对整个输入数据块运行 CMAC 算法，并生成最终的 128 位身份验证标签。

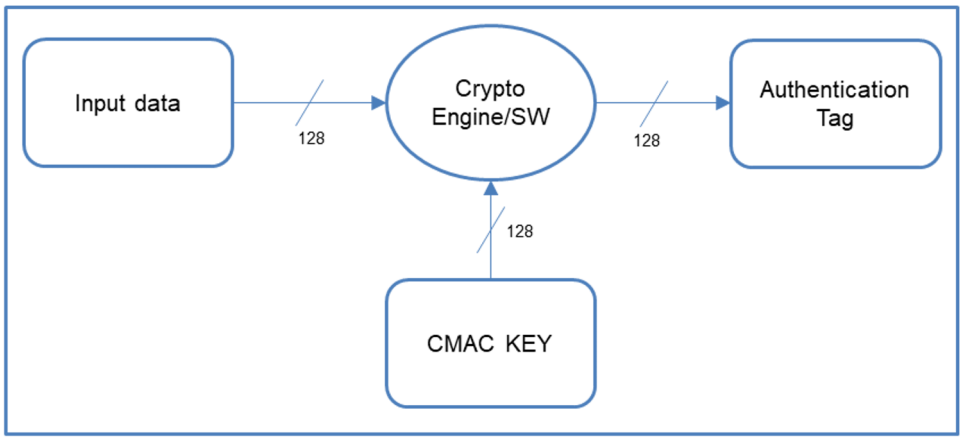

图 3-1. CMAC 工作原理

4 安全闪存启动选项

表 4-1 所示为三个内核上可用的不同主要安全闪存启动选项及其相应的配置。由应用程序代码启动的“扩展安全启动”在节 7 中有相关说明。更多详细信息，请参阅《*TMS320F2838x 技术参考手册*》[1] 中的 *ROM 代码和外设启动* 一章。

表 4-1. 安全闪存启动模式配置详细信息

安全启动选项 (1)	BOOTDEFx/ BOOTMODE 值 (2)	闪存入口点 (3)	CPU1/CPU2 入口地址	CPU1/CPU2 128 位黄金 CMAC 标签位置	CM 入口地址	CM 128 位黄金 CMAC 标签位置
选项 0	0x0A	扇区 0	0x00080000	0x00080002	0x00200000	0x00200004
选项 1	0x2A	扇区 4	0x00088000	0x00088002	0x00210000	0x00210004
选项 2	0x4A	扇区 8	0x000A8000	0x000A8002	0x00250000	0x00250004
选项 3	0x6A	扇区 13	0x000BE000	0x000BE002	0x0027C000	0x0027C004

(1) 可为 CPU1/CPU2/CM 分别选择安全启动选项。
(2) 对于 CPU1，BOOTDEFx 字段是 Zx-BOOTDEF-LOW/Zx-BOOTDEF-HIGH CPU1 USER OTP 存储器位置的一部分。对于 CPU2/CM，BOOTMODE 字段是 CPU1TOCPU2IPCBOOTMODE/CPU1TOCMIPCBOOTMODE 寄存器的一部分，分别由 CPU1 应用程序代码填充。
(3) 安全启动特性仅适用于 Zone1，因此所选闪存扇区必须配置为 Zone1-EXEONLY。此外，无论扇区大小如何，“主要安全闪存启动”仅基于所选扇区的前 16KB 运行。例如，扇区 4 和扇区 8 各为 64KB，但仅考虑前 16KB。

5 安全闪存启动流程

在器件上实现安全闪存启动的过程包含两步：

1. **生成身份验证标签** – 此过程是在器件外部创建映像期间进行的。
   a. C2000™ 或 Arm® 十六进制实用程序使用输入 CMACKEY 以及能够为黄金 CMAC 身份验证标签保留存储空间的 CMAC 应用程序数据结构来对闪存启动代码映像运行 CMAC 算法。更多有关十六进制实用程序的详细信息，请参阅 [3] 和 [4]。
   b. 生成的黄金 CMAC 标签嵌入在十六进制文件中由表 4-1 指定的位置。
   c. 十六进制映像（现在包含黄金 CMAC 标签）被编程到闪存的相应扇区中。
   d. 相应的安全闪存启动模式应根据表 4-1 进行选择并编程到 CPU1 USER OTP 中。
2. **对闪存中的应用程序启动代码进行身份验证** – 此过程在器件内部执行安全闪存启动时进行。
   a. BOOTDEFx/BOOTPINCONFIG 字段被配置为根据表 4-1 选择安全闪存启动选项（在复位时，器件会启动）并对指定的闪存扇区执行 CMAC 算法。
   b. 将由 CMAC 算法生成的标签与位于预编程位置的黄金 CMAC 标签进行比较。
   c. 标签匹配成功后，启动过程将分支到经过身份验证的闪存代码并开始执行。
   d. 如果标签匹配失败，则会对 CPU1/CPU2/CM 采取不同的操作：
      i. 如果是 CPU1，则会将器件复位（代码保持在循环中，并且在看门狗到期时会自动发出 XRSn）。
      ii. 如果是 CPU2，则会在 CPU2TOCPU1IPCBOOTSTS 寄存器中设置安全启动失败标志，将 IPC 命令与安全闪存 CMAC 错误代码一起发送到 CPU1，并且 CPU2 启动代码会循环等待 CPU1 以采取必要操作。还会在 CPU2 的 0x0000 0002 地址位置捕获 CPU2TOCPU1IPCBOOTSTS 寄存器的副本。
      iii. 如果是 CM，则会在 CMTOCPU1IPCBOOTSTS 寄存器中设置安全启动失败标志，将 IPC 命令与安全闪存 CMAC 错误代码一起发送到 CPU1，并且 CM 启动代码会循环等待 CPU1 以采取必要操作。还会在 CM 的 0x2000 0000 地址位置捕获 CMTOCPU1IPCBOOTSTS 寄存器的副本。

NOTE

在计算映像上的身份验证标签以及对映像进行身份验证时，CMAC 算法会将包含黄金标签的存储器地址视为全 1。

6 C2000Ware 示例详细信息

C2000Ware [2] 通过一个示例来说明应用程序的安全闪存启动设置。该示例包括针对每个内核的安全闪存启动应用程序工程。该示例还详细说明了如何对安全闪存启动入口地址 + 16KB 之外的闪存代码进行身份验证。节 7 中提供了关于此定制闪存范围身份验证功能的更多详细信息。该示例假设要进行身份验证的闪存扇区已预先配置为 Zone 1 EXEONLY 并使用默认 CMACKEY 进行身份验证。有关在 CPU1 USER OTP 中对定制 CMACKEY 和其他 DCSM 设置进行编程的详细信息，请参阅 [1] 和 [2]。

C2000Ware 位置：<C2000Ware_安装目录>/driverlib/f2838x/examples/c28x/boot

工程名称：

- boot_ex1_cpu1_cpu2_cm_secure_flash_cpu1
- boot_ex1_cpu1_cpu2_cm_secure_flash_cpu2
- boot_ex1_cpu1_cpu2_cm_secure_flash_cm

包含的文件：

- 源文件 – 包含主应用程序代码
  - 示例：boot_ex1_cpu1_cpu2_cm_secure_flash_cpu1.c
- 十六进制链接器命令文件 – 向 c2000 或 arm hex 实用程序提供整个闪存长度的详细信息
  - 示例：boot_ex1_flash_hex_lnk_cpu1.cmd
- CMAC 密钥文本文件 – 为 c2000 或 arm hex 实用程序提供用户 CMAC 密钥
  - 示例：boot_ex1_user_cmac_key.txt
  - 更多有关 cmac_key 格式的详细信息，请参阅 [3] 和 [4]。

如何运行该示例：

1. 将应用程序加载到 CPU1 闪存中（以及 CPU2 和 CM 应用程序）。
   a. 加载 *.hex 文件，而不是 *.out 文件
2. 断开连接并仅重新连接到 CPU1。
3. 要将器件配置为在启动时执行安全闪存启动：
   a. 仿真启动（建议用于示例/开发）
      i. 在 CCS 存储器窗口中，将 BOOTPINCONFIG 位置 (0x0D00) 设置为 0x5AFFFFFF，并将 BOOTDEF 位置 (0x0D04) 设置为 0x0000000A
   b. 独立启动（建议用于部署）
      i. 对与 BOOTPINCONFIG 和 BOOTDEF 相对应的 CPU1 USER OTP 位置进行编程。若要了解更多信息，请参阅 [1]。
4. 通过 CCS 重置 CPU1，然后点击“Resume”。
5. 观察 controlCARD 上的 LED 指示灯是否指示已成功。
   a. 当所有三个内核都成功地安全启动并对它们的完整闪存内容进行身份验证时，三个 LED 指示灯（每个内核一个）将闪烁。
6. 对于不使用 controlCARD 的情况，请注意以下基于 CPU 子系统的 GPIO 切换开关：
   a. CPU1 – GPIO31
   b. CPU2 – GPIO34
   c. CM – GPIO145

生成黄金 CMAC 标签的应用程序代码要求：

用于安全闪存启动选项 0 的 CPU1/CPU2 黄金 CMAC 标签存储器分配

```
// CPU1/CPU2 的实现情况
#pragma RETAIN(cmac_sb_1)
#pragma LOCATION (cmac_sb_1, 0x080002)
const char cmac_sb_1[8] = {0};
```

用于安全闪存启动选项 0 的 CM 黄金 CMAC 标签存储器分配

```
#pragma RETAIN(cmac_sb_1)
#pragma LOCATION (cmac_sb_1, 0x00200004)
const uint8_t cmac_sb_1[16] = {0};
```

常量字符/无符号整数定义会为黄金 CMAC 标签分配存储器。如需更多信息，请参阅节 6 中的示例：

- 变量命名必须为以下之一：cmac_sb_1、cmac_sb_2、cmac_sb_3、cmac_sb_4
  - 在《*TMS320C28x 汇编语言工具用户指南*》[3] 中可找到更多有关 C28x 的详细信息
  - 在《*ARM 汇编语言工具用户指南*》[4] 中可找到更多有关 CM 的详细信息
- 使用 LOCATION pragma 为 CMAC 黄金标签指定预期身份验证范围内的地址。对于 CPU1/CPU2，此地址必须为入口地址 + 2，对于 CM，此地址必须为入口地址 + 4。
- 保持变量初始化为零。

使用十六进制实用程序时的应用程序设置：

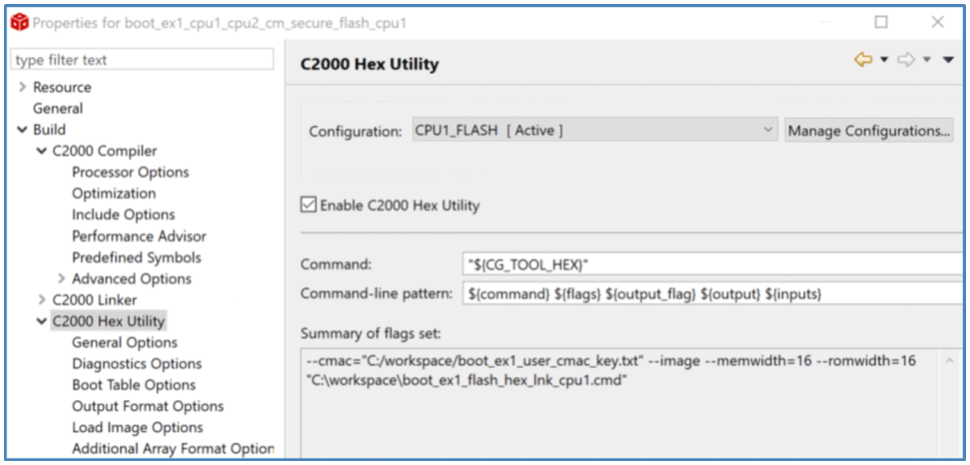

图 6-1. 为 CMAC 启用十六进制实用程序后的 CPU1 示例属性

每个内核工程都使十六进制实用程序能够生成黄金 CMAC 标签（请参阅图 6-1）。标签包括：

- “--cmac”，提供用户 CMAC 密钥文本文件的路径
- “--image”、“--memwidth”和“--romwidth”，其中设置了 mem/rom。CPU1/CPU2 的此设置应为 16，CM 的此设置应为 8
- 对应内核的闪存十六进制链接器命令文件的路径。

7 对超过 16KB 的闪存代码进行身份验证

“安全闪存启动”仅对从入口地址开始的前 16KB 闪存扇区 进行身份验证。为了对闪存的其他扇区进行身份验证，用户应用程序必须直接调用安全闪存启动 CMAC API。

通过使用十六进制实用程序，它支持为四个闪存入口地址中的每一个 + 16KB 和 1 个定制闪存范围生成黄金 CMAC 标签。定制闪存范围可配置为能够在定制地址范围内进行 CMAC 身份验证。如有需要，此范围可以是所有闪存扇区的长度。

用于定制闪存范围身份验证的 CPU1/CPU2 应用程序 CMAC 结构

```
struct CMAC_TAG
{
   char tag[8];
   uint32_t start;
   uint32_t end;
}
```

用于完整闪存范围身份验证的 CPU1/CPU2 黄金 CMAC 标签存储器分配

```
#pragma RETAIN(cmac_all)
#pragma LOCATION (cmac_all, 0x087002)
const struct OMAC_TAG cmac_all = {{0}, 0x0, 0x0};
```

用于定制闪存范围身份验证的 CM 应用程序 CMAC 结构

```
struct CMAC_TAG
{
   uint8_t tag[16];
   uint32_t start;
   uint32_t end;
}
```

用于完整闪存范围身份验证的 CM 黄金 CMAC 标签存储器分配

```
#pragma RETAIN(cmac_all)
#pragma LOCATION (cmac_all, 0x00204004)
const struct OMAC_TAG cmac_all = {{0}, 0x0, 0x0};
```

创建一个名为“cmac_all”的结构，用于创建定制 CMAC 身份验证范围。

- 使用 LOCATION pragma 为 CMAC 黄金标签指定预期身份验证范围内的任何地址。（CMAC 黄金标签越接近身份验证起始地址，CMAC 算法的执行速度越快）。
- 让“tag”结构元素始终初始化为零。
- 初始化“start”和“end”结构元素以设置定制范围。如果两者都为零，则器件内核闪存的全部长度都将接受身份验证，包括“主要安全启动”的 16KB 存储器范围。
- 更多有关应用程序 CMAC 变量/结构的详细信息，请参阅 [3] 和 [4]。

CPU1 安全闪存 CMAC 身份验证 API

```
applicationCMACStatus = CPU1BROM_calculateCMAC (CMAC_AUTH_START_ADDRESS,
                                                CMAC_AUTH_END_ADDRESS,
                                                CMAC_AUTH_TAG_ADDRESS);
```

在应用程序中，将 F2838x 安全区域代码符号库包含到工程中（位于 C2000Ware [2] 中的 <C2000Ware_安装目录>/libraries/boot_rom/f2838x 位置），并调用相应内核的安全闪存启动 CMAC API。以上示例显示了在 CPU1 上进行的示例 API 调用。

- CMAC_AUTH_TAG_ADDRESS 应该与提供给 LOCATION pragma 的内容匹配
- CMAC_AUTH_START_ADDRESS 和 CMAC_AUTH_END_ADDRESS 应该与提供给“cmac_all”结构的内容匹配。此外，需要注意起始地址和结束地址应对齐到 128 位，这很重要。
- 例如，用于对 F2838x CPU1 闪存全部长度进行身份验证的起始地址和结束地址为：
  - 起始：0x00080000

  - 结束：0x000C0000
- 然后应在用户应用程序中相应地检查和处理从安全闪存启动 CMAC API 返回的状态。
- 更多有关安全闪存 CMAC 身份验证 API 的详细信息，请参阅 [1] 中的 *ROM 代码和外设启动* 一章 。

NOTE

即使以上示例中的结束地址实际为 0x000BFFFF，也必须提供 0x000C0000，以便结束地址对齐到 128 位。

8 调试资源

表 8-1. 安全闪存启动调试场景

场景	行为
CPU1 中的安全启动失败	独立启动：器件复位。 仿真启动：CPU1 在地址范围 0x3FB13C – 0x3FB142 内停止
CPU2 中的安全启动失败	CPU2TOCPU1IPCBOOTSTS (1) 寄存器的 Bit21 将被设置。 CPU2 向 CPU1 发送带有安全闪存 CMAC 错误代码的 IPC 命令。
CM 中的安全启动失败	CMTOCPU1IPCBOOTSTS (2) 寄存器的 Bit21 将被设置。CM 向 CPU1 发送带有安全闪存 CMAC 错误代码的 IPC 命令。
CPU1 的安全启动是否成功运行？	位于 0x0000 0002 地址位置的 CPU1 BootROM 状态 Bits7:0 将反映 0x3。
CPU2 的安全启动是否成功运行？	CPU2TOCPU1IPCBOOTSTS (1) 寄存器的 Bits7:0 将反映 0x3。
CM 的安全启动是否成功运行？	CMTOCPU1IPCBOOTSTS (2) 寄存器的 Bits7:0 将反映 0x3。

1. 在位于 CPU2 的 0x0000 0002 地址位置也捕获了相同的信息。
2. 在位于 CM 的 0x2000 0000 地址位置也捕获了相同的信息。

9 其他信息和注意事项

- 虽然不推荐，但如果对 CPU2/CM 而不是对 CPU1 执行安全闪存启动，那么在将 CPU2/CM 解除复位之前，必须从 CPU1 为 Z1 OTP CMACKEY 执行虚拟加载。虚拟加载是通过读取 CPU1 USER OTP 中的 0x78018-0x7801F 位置来完成的。
- 同样，如果在没有对 CPU1 运行安全闪存启动模式的情况下使用 CMAC 身份验证 API，那么在调用这些 API 之前，必须从 CPU1 为 Z1 OTP CMACKEY 执行虚拟加载。
- 在对 CPU1 使用安全闪存启动时，建议不要对 BOOTDEF 表中配置的同一扇区使用正常（非安全）闪存启动模式。
- 若要对超过 16KB 的闪存代码进行身份验证：
  - 128 位黄金 CMAC 标签必须存储在执行计算的存储器地址范围内。
  - 黄金 CMAC 标签的起始地址必须与 32 位边界对齐。
- 启动模式设置位于一次性可编程 (OTP) 闪存中，因此建议在冻结与启动相关的配置之前使用仿真启动模式进行试验。更多有关仿真启动的信息，请参阅 *《TMS320F2838x 技术参考手册》* [1] 中的 *ROM 代码和外设启动* 一章。

10 参考文献

1. 德州仪器 (TI)： *《TMS320F2838x 实时微控制器技术参考手册》*
2. 适用于 C2000 实时 MCU 的 C2000Ware
3. 德州仪器 (TI)： *《TMS320C28x 汇编语言工具 v20.2.0.LTS 用户指南》*
4. 德州仪器 (TI)： *《Arm 汇编语言工具 v20.2.0.LTS 用户指南》*
5. TMS320F28338D 产品页面

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265