

Application Report

C2000™ 唯一器件编号



Salvatore Pezzino, Joe Prushing, David Foley

摘要

本文档介绍了在制造期间存储在每个器件中的 32 位值。其中介绍了将此值用作唯一器件标识符的方法，以及与使用此值生成加密密钥相关的限制。

内容

1 引言.....	2
2 A 类器件.....	2
2.1 限制.....	2
3 B 类器件.....	3
3.1 限制和可变性.....	3
4 器件表.....	4
5 修订历史记录.....	4

表格清单

表 4-1. C2000 器件上的唯一 ID 位置.....	4
--------------------------------	---

商标

C2000™ is a trademark of Texas Instruments.

所有商标均为其各自所有者的财产。

1 引言

很多 C2000™ 器件包含唯一的器件编号，应用可以使用该编号来增强安全解决方案。该唯一器件编号有多种用途。下面这些示例说明了唯一器件编号的用途。

- 防止使用定期读回和比较进行代码克隆
- 对程序或数据进行加密或解密的初始化矢量 (IV)
- 身份验证的 IV
- 通信 (广播) 中的器件识别
- 数据完整性算法的种子，例如，循环冗余校验 (CRC)

随着 C2000 技术和器件的进步，唯一器件编号的实现也在不断演变。有两类器件，它们被区分为 A 类和 B 类以供以下讨论。

A 类器件：

- F280x
- F2802x
- F2803x
- F2805x
- F2806x
- F2823x 和 F2833x

B 类器件：

- F2807x
- F2837x
- F28004x
- F2838x
- F28002x

2 A 类器件

对于 A 类器件，器件编号是伪唯一的。“伪”一词旨在明确传达 TI 不保证此值对于每个器件都是唯一的，但它通常应该是唯一的。

提供的 32 位值可被视为两个 16 位字。为获得随时间推移的最佳唯一性，应使用所有 32 位。如果只需要 16 位，TI 建议将最低有效字 (LSW) 和最高有效字 (MSW) 通过异或 (XOR) 方法放在一起。如果无法做到这一点，则应使用 LSW，因为单纯 MSW 可能无法包含足够的材料可变性来满足所需的要求。如需更多信息，请参见节 2.1 和节 2.1.1。

2.1 限制

必须传达一些限制，才能正确评估此值是否适合客户应用中的预期目的。

2.1.1 可变性

32 位值不是随机生成的伪数，而是基于简单的序列化算法。几乎同时制造的器件可能具有相同或相似的 MSW，但通常应具有唯一的 LSW。在典型情况下，LSW 可能会在数百个或数千个器件内重复。通过同时使用 MSW 和 LSW，器件编号重复的可能性大大降低。

2.1.2 静态位

32 位值中的某些位通常具有固定值零。静态位会减少 32 位数字的可能值。MSW 中有 1 个静态位，LSW 中有 4 个静态位。

2.1.3 长期可靠性

不保证 32 位值在器件的整个生命周期内在所有工作条件下都保持一致。如果使用该值，则应将其复制到片上非易失性位置，例如用户一次性可编程 (OTP) 存储器或闪存。

2.1.4 未经过测试

出厂测试期间，不会基于 32 位值拒绝器件。结果是多个器件可能被编程为具有共同值，特别是所有位均为零或一，或一些其他非标准值。

3 B 类器件

B 类器件与 A 类器件具有不同的特性。B 类器件在 OTP 中提供用于器件识别的 UID_REGS 寄存器。UID_REGS 寄存器包含一个 256 位值，该值由伪随机和顺序值组成。该值可作用于代码加密的种子。前 192 位是伪随机值，接下来的 32 位是顺序值，最后 32 位是前 224 位的 Fetcher 校验和值。

32 位顺序值是 UID_UNIQUE 器件识别寄存器，对于特定器件系列（例如 F2807x、F2837x 等）的所有器件都是唯一的。因此，256 位的值也是唯一的。

3.1 限制和可变性

必须传达一些限制，才能正确评估此值是否适合客户应用中的预期目的。

不保证 192 位伪随机值具有特定程度的熵。因此，应仔细考虑将伪随机值用作加密密钥，以防止应用必须防范的威胁级别。在密码学中用作 IV 是可以接受的，前提是 IV 无需使用熵。

32 位 UID_UNIQUE 值不是随机生成的伪数，而是基于简单的序列化算法。尽管 UID_UNIQUE 值对于特定器件系列中的某个单元是唯一的，但在某些情况下，跨器件系列的两个单元将使用同一 UID_UNIQUE 编号。如果需要整个器件系列保持唯一，UID_UNIQUE 值应与器件数据表中列出的 PARTIDH 值交叉参考。

4 器件表

表 4-1 列出了可从中读取多个器件系列的 MSW 和 LSW 的存储器映射地址。

表 4-1. C2000 器件上的唯一 ID 位置

器件系列	MSW 位置	LSW 位置
F24x 和 F240x	不适用	不适用
F280x	0x000809	0x000808
F2802x	0x000901	0x000900
F2803x	0x000901	0x000900
F2805x	0x3D7FDB	0x3D7FDA
F2806x	0x000901	0x000900
F2823x 和 F2833x	0x000901	0x000900
F2807x ⁽¹⁾	0x0703CD	0x0703CC
F2837x ⁽¹⁾	0x0703CD	0x0703CC
F28004x ⁽¹⁾	0x0703CD	0x0703CC
F2838x ⁽¹⁾	0x07020D	0x07020C
F28002x ⁽¹⁾	0x0701F5	0x0701F4

(1) 有关此 UID_UNIQUE 寄存器的更多信息，请参阅器件数据表和技术参考手册。

5 修订历史记录

注：以前版本的页码可能与当前版本的页码不同

Changes from Revision A (June 2019) to Revision B (September 2020)	Page
• 更新了整个文档中的表、图和交叉参考的编号格式。.....	2
• 对节 1 进行了更新。.....	2
• 对节 4 进行了更新.....	4

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

Copyright © 2022，德州仪器 (TI) 公司