AN2004
应用笔记

UM32x13x EEPROM 配置说明

版本：V1.0

Unicmicro



广芯微电子（广州）股份有限公司

http://www.unicmicro.com/

条款协议

本文档的所有部分，其著作产权归广芯微电子（广州）股份有限公司（以下简称广芯微电子）所有，未经广芯微电子授权许可，任何个人及组织不得复制、转载、仿制本文档的全部或部分组件。本文档没有任何形式的担保、立场表达或其他暗示，若有任何因本文档或其中提及的产品所有资讯所引起的直接或间接损失，广芯微电子及所属员工恕不为其担保任何责任。除此以外，本文档所提到的产品规格及资讯仅供参考，内容亦会随时更新，恕不另行通知。

1. 本文档中所记载的关于电路、软件和其他相关信息仅用于说明半导体产品的操作和应用实例。用户如在设备设计中应用本文档中的电路、软件和相关信息，请自行负责。对于用户或第三方因使用上述电路、软件或信息而遭受的任何损失，广芯微电子不承担任何责任。
2. 在准备本文档所记载的信息的过程中，广芯微电子已尽量做到合理注意，但是，广芯微电子并不保证这些信息都是准确无误的。用户因本文档中所记载的信息的错误或遗漏而遭受的任何损失，广芯微电子不承担任何责任。
3. 对于因使用本文档中的广芯微电子产品或技术信息而造成的侵权行为或因此而侵犯第三方的专利、版权或其他知识产权的行为，广芯微电子不承担任何责任。本文档所记载的内容不应视为对广芯微电子或其他人所有的专利、版权或其他知识产权作出任何明示、默示或其它方式的许可及授权。
4. 使用本文档中记载的广芯微电子产品时，应在广芯微电子指定的范围内，特别是在最大额定值、电源工作电压范围、热辐射特性、安装条件以及其他产品特性的范围内使用。对于在上述指定范围之外使用广芯微电子产品而产生的故障或损失，广芯微电子不承担任何责任。
5. 虽然广芯微电子一直致力于提高广芯微电子产品的质量和可靠性，但是，半导体产品有其自身的具体特性，如一定的故障发生率以及在某些使用条件下会发生故障等。此外，广芯微电子产品均未进行防辐射设计。所以请采取安全保护措施，以避免当广芯微电子产品在发生故障而造成火灾时导致人身事故、伤害或损害的事故。例如进行软硬件安全设计（包括但不限于冗余设计、防火控制以及故障预防等）、适当的老化处理或其他适当的措施等。

Unicmicro

 Copyright © 2023 广芯微电子（广州）股份有限公司

目录

1 摘要 1
2 EEPROM 简介 1
3 EEPROM 配置说明 1
4 版本维护 3

Unicmicro

 Copyright © 2023 广芯微电子（广州）股份有限公司

1 摘要

本篇应用笔记主要介绍 UM32x13x EEPROM 配置说明。

本篇应用笔记主要包括：

- EEPROM 简介
- EEPROM 配置说明

2 EEPROM 简介

UM32x13x 系统中 EEPROM 共分为两块：EEPROM1 和 EEPROM2，每块 EEPROM 含有 512 Bytes。

EEPROM1 的地址空间为：0x0001_0000 ~ 0x0001_0200。

EEPROM2 的地址空间为：0x0001_0200 ~ 0x0001_0400。

EEPROM 特性：

- EEPROM1 和 EEPROM2 可以作为普通数据存储区域存储数据，也可以作为软件程序存储空间，CPU 可以在 EEPROM 区域进行取指令。
- EEPROM1 和 EEPROM2 只能通过 Sector Erase 操作进行擦除，不能通过 Chip Erase 擦除。
- 对 Flash 的 Main 区的 Chip Erase 操作，不能将 EEPROM 空间内的数据擦除。
- 对 EEPROM 空间发起 Chip Erase 操作不会成功，且会触发 EFC 模块中的异常中断。

3 EEPROM 配置说明

EEPROM2 与 EEPROM1 相比，空间最后 5 个 Word，有特殊的定义。当其值等于特定的花样值时，芯片在经过外部复位或掉电复位后，会产生特定的配置效果。

下面对 EEPROM2 最后 5 个 WORD 的花样值进行描述：

1. SWD_READ_DISABLE，地址：0x0001_03EC。当此地址数据为 0x5389BCEA 时，且经过外部 IO 复位（RESETN）或者掉电复位后，花样值生效，开启对 Flash 中所有数据进行保护模式。在这种保护模式下，SWD 读取 Flash 中任何区间的数据，都将返回伪数据 0xdeaddead。只有在对 Main 区发起 Chip Erase 后，读取 Main 区的数据才会为真实的数据。
2. KEY_RD_DISABLE，地址：0x0001_03F0。此地址的配置位为 Flash 程序加解密 KEY 的保护花样。当其值等于 0x55AAAA55 时，读取 PRIVATE_KEY 花样值，将会返回 0xdeaddead，即起到对 PRIVATE_KEY 花样值的保护作用。

Copyright © 2023 广芯微电子（广州）股份有限公司

3. FLASH_CRYPT_EN，地址：0x0001_03F4。此地址的配置为 Flash 中程序的加解密配置位。UM32x13x 支持 Flash 中程序加解密配置，且加解密模式共有两种模式选择。
   - 加解密模式 1：当 FLASH_CRYPT_EN 的值为 0x55AAAA55 时，芯片开启加解密模式 1。加解密模式 1 的行为为数据进入 Flash 前，进行加密，数据从 Flash 中被读取，进行解密。加解密的密钥，来自 PRIVATE_KEY 花样。使用这种模式时，Flash 中存储的数据均为密文，通过 EFC 读取解密后，会转变为明文，可以有效的提升对芯片 Flash 中存储数据的物理手段攻击。
   - 加解密模式 2：当 FLASH_CRYPT_EN 的值为 0xAA5555AA 时，芯片开启加解密模式 2。在加解密模式 2 下，在芯片系统运行 Boot 程序阶段（未写 SCU 中的 REMAP 寄存器），数据在进入 Flash 中为明文进入和读取，EFC 不对数据进行加解密操作。当芯片系统运行在用户程序阶段，即 Boot 程序已经完成引导，且写 SCU 中的 REMAP 寄存器进行软复位时，则 EFC 开启对 Flash 中数据的加解密模式。加解密的密钥，来自 PRIVATE_KEY 花样。使用这种模式时，使用 Boot 烧录，需要对烧录的软件程序数据先进行加解密操作，且加解密的算法与密钥需要与 PRIVATE_KEY 花样一致，然后再烧录，可以有效的保护数据在烧录厂存储环节不被泄露。
4. PRIVATE_KEY，地址：0x0001_03F8。此地址内存放 Flash 加解密的密钥。Flash 加解密只对 Flash 的 64Kbytes 的 Main 区起作用，不对 EEPROM 区、NVR 区和 Boot 区起作用。当 KEY_RD_DISABLE 花样值为 0x55AAAA55，且芯片经过外部 IO 复位（RESETN）或掉电复位后，PRIVATE_KEY 值将被保护。读取 PRIVATE_KEY 值将返回 0xdeaddead 的 Dummy 值。
5. OTP_C_EN，地址：0x0001_03FC。此值为 EEPROM2 区是否可以擦写的配置花样。当此地址存储的值为 0x55AAAA55 时，EEPROM2 区域将无法被擦写，即 EEPROM2 区域将被锁定，内部的值将无法被擦除或者重写，EEPROM2 表现和 ROM 一样。

Unicmicro

 Copyright © 2023 广芯微电子（广州）股份有限公司

4 版本维护

版本	日期	描述
V1.0	2023.12.27	初始版

Unicmicro

Copyright © 2023 广芯微电子（广州）股份有限公司