Application Note

TKScope 对 LPC1300 系列芯片的完整编程/加密方法

AN05220055 V1.00 Date: 2011/12/02 产品应用笔记

类别	内容
关键词	TKScope 仿真器 LPC1300 Flash 加密 在线编程 烧写
特 性	**1. 支持片内 Flash 在线编程；** **2. 支持编程时使用不同 CRP 等级加密芯片。**
摘 要	介绍如何使用 TKScope 仿真器、K-Flash 在线编程并加密 LPC1300

TKScope®

目　录

1. 背景资料

1.1 LPC1300 的加密机制

LPC1300 系列是 NXP 采用 ARM 公司的 Cortex-M3 内核设计并生产的 MCU，由于其性能卓越、简单易用、功耗低、以及能显著降低所有 8 位/16 位应用的代码长度，其价值和易用性比现有的 8 位/16 位微控制器更胜一筹，被广大工程师应用于各种设计场合。

为了保障用户代码安全，LPC1300 提供了加密机制。其工作机理是通过在片内 Flash 地址 0x000002FC 处写入特定的加密数值来实现不同的加密等级，如表 1.1 所示。

表 1.1　LPC1300 加密等级

CRP 等级	0x000002FC 内容	SWD	ISP	解除加密方法
NO_ISP	0x4E697370	使能	禁用	-----
CRP1	0x12345678	禁用	使能	ISP 擦除整片
CRP2	0x87654321	禁用	使能	ISP 擦除整片
CRP3	0x43218765	禁用	禁用	无法解除

1.2 带来的风险与不便

由于该地址(0x000002FC)在用户 Flash 地址范围内；在实际使用过程中，由于工程配置不当，工程师们经常会误加密而导致 JTAG/SWD 接口被锁死，此时必须通过 ISP 方式擦除整片 Flash 才能继续使用仿真器仿真调试。这意味着需要从硬件电路板引出 UART 接口，增加一部分不必要的硬件电路，对已经完成生产的产品带来不便。

更有甚者，甚至误提高加密等级至最高(CRP3)而致使 ISP 也被禁止，无法进行任何调试或改写片内 Flash 内容的操作。

但有一些用户反而可能希望使用加密功能，比如在最终的产品生产烧写时。目前普通的 ARM 仿真器仅仅能实现将用户程序的完整代码下载到 Flash 中，如果需要加密，要求用户必须手动在代码中加入加密数值。这需要工程师非常耐心地详细阅读英文版数据手册，并花大量的时间和精力编写和调试代码！

1.3 TKScope 提供完整的解决方案

作为国内嵌入式仿真器行业中最富有影响力的领导品牌，TKScope 嵌入式智能仿真开发平台率先针对以上两种问题提供了完整的解决方案。TKScope 不仅支持在研发阶段避免误加密；同时也提供了最终的生产烧写时提供不同加密等级的加密；也可为量产提供完整的编程解决方案。

2. TKScope 仿真器的支持

TKScope 嵌入式智能仿真开发平台是广州致远电子有限公司推出的高性能通用型综合仿真开发平台；支持仿真全系列的 8051、ARM、DSP、AVR、C166、C251、MX 等内核；与当前全部主流 IDE 环境无缝嵌接，如 Keil、ADS、IAR、CCS、RealView、AVRStudio、TKStudio 等，并具备其高级调试功能；同时，TKScope 内嵌 64 路专业的逻辑分析仪，zlgLogic 高级软件全面支持。TKScope 系列仿真器中支持 NXP 公司 LPC1300 系列芯片的仿真和烧写的具体型号有：K8、K9、DK9、DK10、AK100。

同时，TKScope 提供独立的 K-Flash 在线编程软件，用户烧写芯片不再依赖于 IDE 环境，可以直接使用 K-Flash 软件烧写最终的文件。K-Flash 具备良好的易操作性、文件加密字同时烧写的功能、先进的工程管理模式，这些都为用户在线量产编程提供了有力的条件。

图 2.1　K-Flash 软件

3. 详细操作指南

本文主要介绍 TKScope 编程加密 LPC1300 系列的 LPC1343 芯片时，需要特别注意的设置选项，其它详细说明请参阅《TKScope 嵌入式智能仿真开发平台仿真 ARM 快速入门》。主要的配置项为图 3.1 的【硬件选择】和【程序烧写】两项。

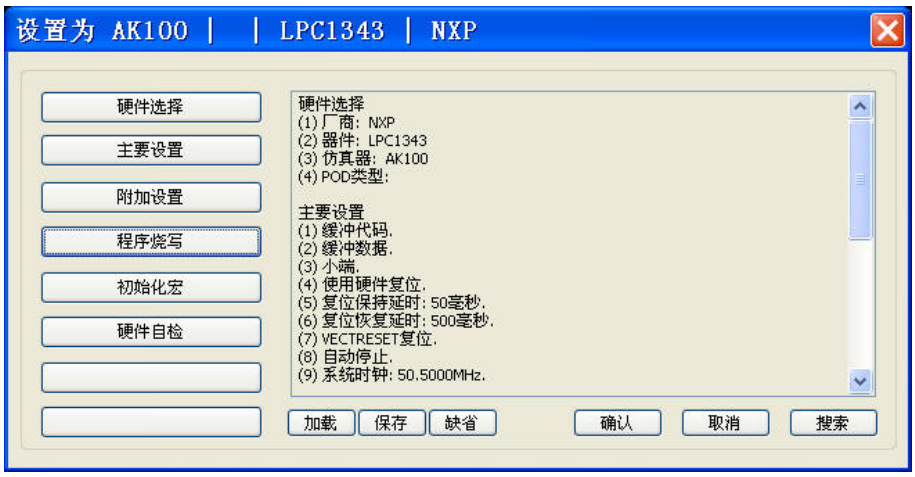


图 3.1　TKScope 硬件选择界面

3.1　硬件选择

TKScope 仿真器设置界面中，【硬件选择】选项设置如图 3.2 所示。在右上角的器件过滤窗口输入 LPC1343，系统会自动找到该芯片，根据所用的具体仿真器型号选择芯片下的仿真器型号即可。注意：一定要正确选择芯片型号及仿真器型号。退出后，点击图 3.1 中的【缺省】按钮以加载缺省的设置。

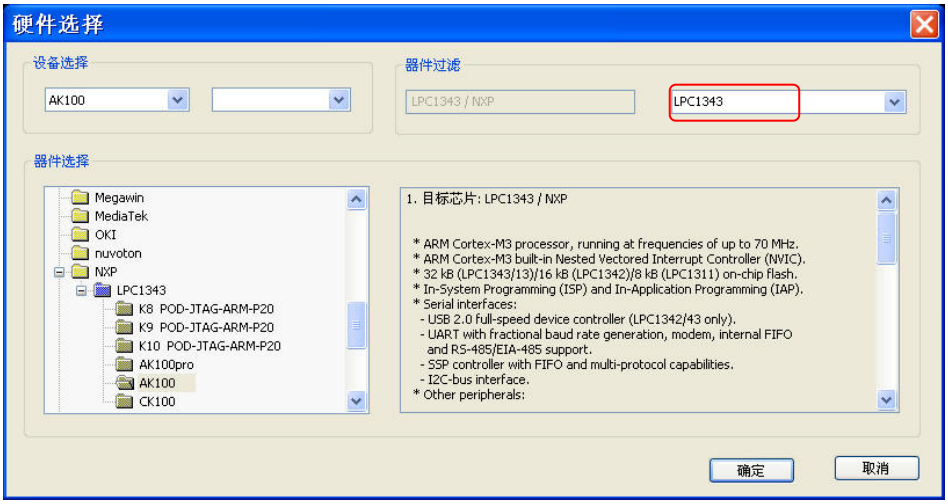


图 3.2　TKScope 硬件选择界面

3.2　程序烧写

TKScope 仿真器设置界面中，【程序烧写】选项设置如图 3.3 所示。注意：如果用户选择在 Flash 中调试，必须选中【编程 Flash】【验证 Flash】选项，同时选择【整片擦除】或【扇区擦除】。如果用户选择在 RAM 中调试，不必选中【编程 Flash】选项。

LPC1343 芯片内部集成 32KBytes 的 Flash 程序存储空间，当正确选择芯片后，系统会自动调用 Flash 算法文件。

TKScope 不仅为 LPC1343 片内 Flash 编程提供了相应的编程算法，而且还提供 Flash【选项】功能，如图 3.3。点击【选项】按钮后，可进入【选项】界面对 LPC1343 选项数据进行配置。

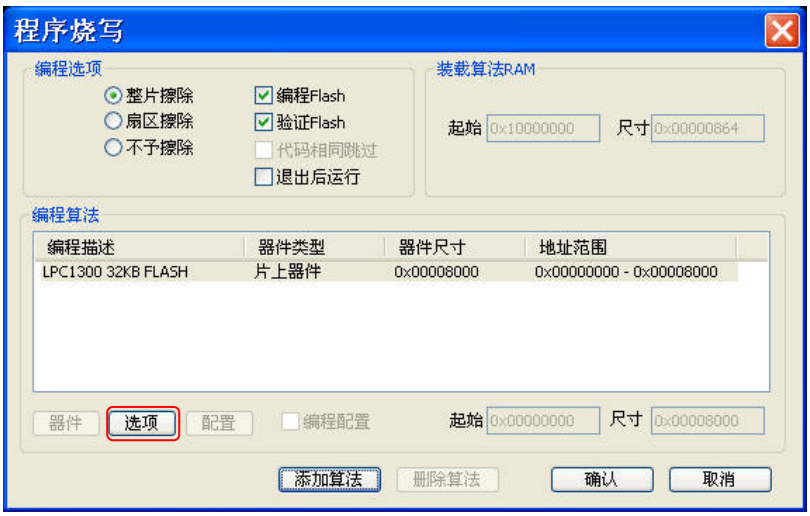


图 3.3　TKScope 程序烧写界面

3.3 加密选项配置

LPC1300 系列芯片 Flash 配置选项主要为芯片加密选项。虽然该选项用户可以在自己的程序代码中进行设置（地址为 0x000002FC）；但是 TKScope 提供了更为直观的图形化界面，更加方便用户设置。下面将介绍各选项的作用。

3.3.1　Violation 标签

Violation 标签用于配置是否由 TKScope 控制选项数据的编程。

TKScope 缺省使用选项界面的数据，而不是用户代码中的数据，这样保证用户在编程时不会误烧加密位而导致芯片无法恢复，如图 3.4 所示。即如果用户希望由 TKScope 控制加密级别，则勾选【Volation】选项。

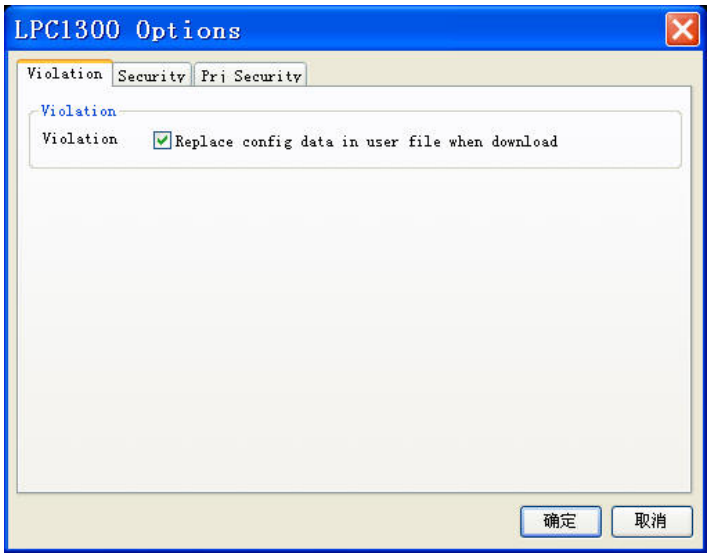


图 3.4　烧写 TKScope 界面中的配置数据

当用户选择使用用户代码中的选项数据时，需要按照图 3.5 操作。由于用户代码中的选项数据不可预计，可能包含加密位，因此这个操作需要不可恢复加密位密码。即如果用户希望自行在代码中配置加密级别，则不勾选【Volation】选项。

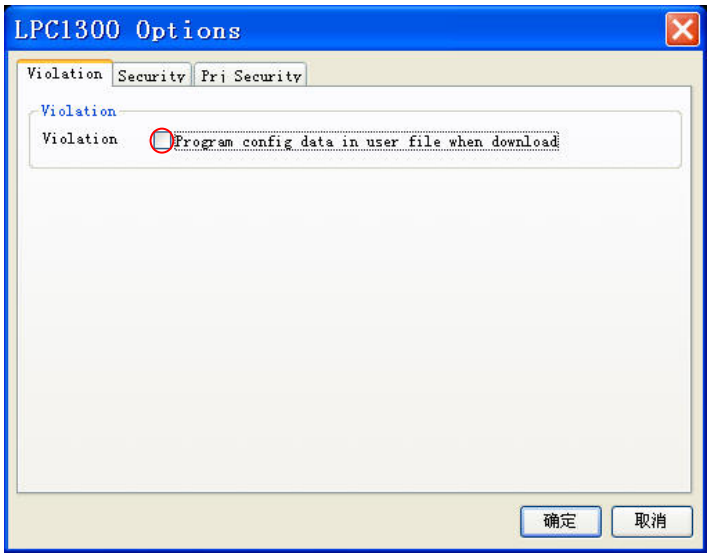


图 3.5　烧写用户代码中的配置数据

3.3.2　加密级别配置

LPC1343 包含 3 级加密：CRP1、CRP2、CRP3，使能任意一级加密都将导致 JTAG 被锁死。该加密级别在【Security】标签中配置，如图 3.6。有关各加密级别的具体含义，请参考数据 LPC1343 的用户手册。

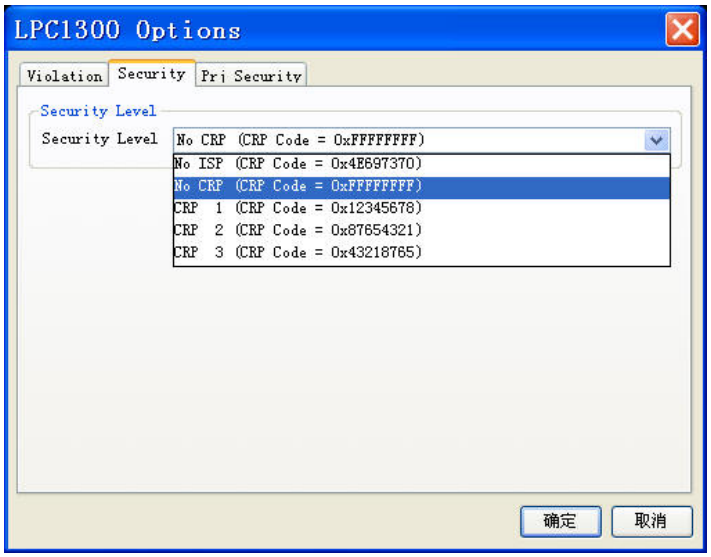


图 3.6　配置 LPC1343 的加密级别

注意！一旦使能加密，JTAG 接口将被禁用，TKScope 仿真器将无法连接调试，用户必须慎重操作!!! 为了避免用户误操作而加密，默认情况下该选项是不可配置的。如果用户确定要对其进行配置，必须先配置【Prj Security 标签】下的【Flash 安全】组！详细的配置说明请见后面章节。

3.3.3　工程安全

该配置用于防止配置信息被其他人读取或修改。比如在使用 TKScope 进行批量在线 Flash 烧写过程中，研发工程师可以提前设置好 LPC1343 的配置信息，然后再将工程交由生产线的工人进行烧写。为避免工人在烧写过程中误操作，研发工程师可以预先锁定 LPC1343 的配置信息；对于一些敏感的配置，也可对其进行隐藏。

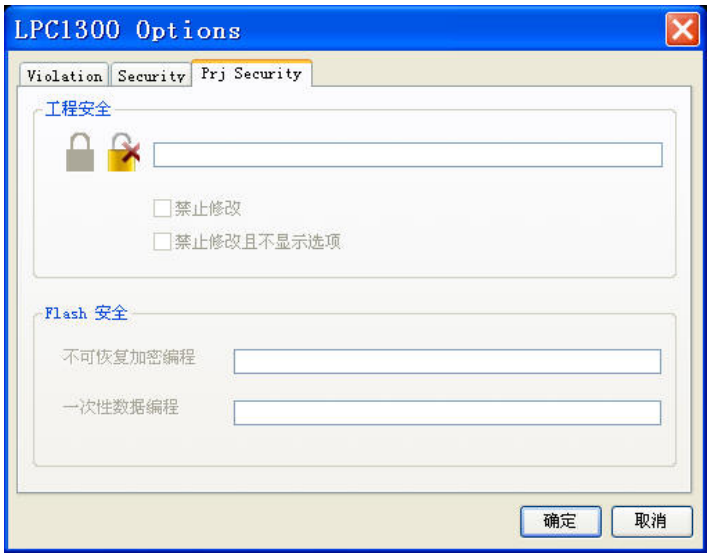


图 3.7　工程配置

1、密码的创建与删除

在使能工程安全之前，必须预先创建密码，该密码用于决定用户是否有权限配置工程安全相关的选项。点击图 3.7 中 图标，弹出新建密码窗口，如图 3.8 所示。

图 3.8　新建工程密码

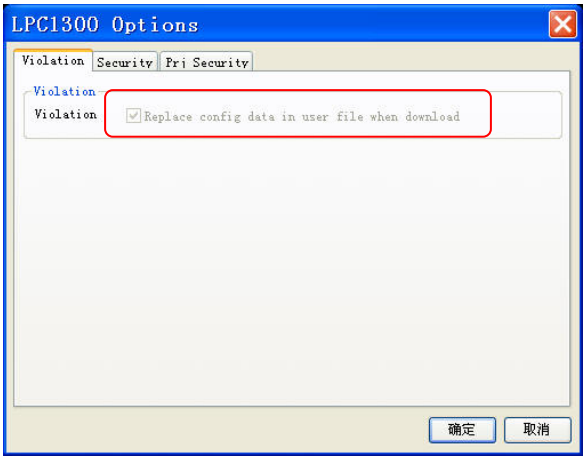
如果用户忘记密码，可点击 按钮删除密码，删除密码后将复位所有的配置选项！

图 3.9　删除密码

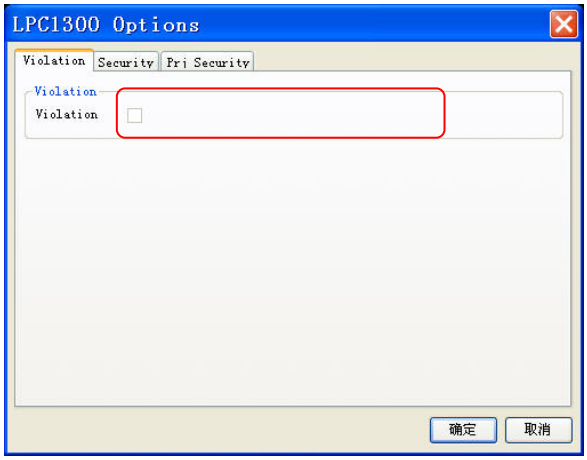
2、工程安全配置

仅当工程密码设置完毕后，【禁止修改】和【禁止修改且不显示选项】才有效。

- 禁止修改选项：配置是否禁止修改【Violation 标签页】和【Security 标签页】的所有选项，配置效果如图 3.10 所示；
- 禁止修改且不显示选项：配置是否禁止修改和显示【Violation 标签页】和【Security 标签页】的所有选项，配置效果如图 3.10 所示。



选择“禁止修改”



选择“禁止修改且不显示选项”

图 3.10　选择“禁止修改”或“禁止修改且不显示”

3.3.4 Flash 安全

该组包含两组配置，用于控制是否允许对不可恢复的配置数据和一次性编程的配置数据进行编程配置。

- 不可恢复加密编程：配置是否允许对芯片中涉及加密类型的配置数据进行编程；
- 一次性数据编程：配置是否允许对芯片中的一次性编程配置数据进行编程。

1. 不可恢复加密编程

【不可恢复加密编程】主要用于一些与芯片加密相关的配置数据的编程。这些加密配置一旦使能，虽然可以避免 Flash 中的代码或数据被恶意读出；但同时带来的问题是 JTAG/SWD 接口将被禁用，无法再使用 TKScope 仿真器进行连接调试。

为避免用户误操作，TKScope 要求用户在使能这些选项之前必须先确认。确认的方法为输入特定的安全密码：123456，如图 3.11 所示。当用户输入正常后，TKScope 即认为用户已经知道相应的风险，才允许用户进行相应的配置。

图 3.11 输入密码 123456

2. 一次性数据编程

【一次性数据编程】主要用于类似 OTP(一次编程)配置数据的编程。这些配置数据仅仅可改写一次。一旦改写，后续将无法再进行任何修改。

为避免用户误操作，TKScope 要求用户在使能这些选项之前必须先确认。确认的方法为输入特定的安全密码：234561，如图 3.12 所示。当用户输入正常后，TKScope 即认为用户已经知道相应的风险，才允许用户进行相应的配置。

图 3.12　输入密码 234561

4. 小结

本文主要介绍TKScope编程LPC1343芯片的一些注意事项，还介绍了如何使用TKScope对芯片进行不同等级的加密。

综上所述，TKScope 嵌入式智能仿真开发平台不仅为使用 LPC1300 系列芯片的工程师提供了完善的仿真与调试手段，而且也提供了非常人性化的 Flash 编程功能；尤其是除了提供一般 Flash 数据烧写功能外，还提供了完整的器件配置编程。正是因为提供了这些完善的仿真与编程功能，越来越多的工程师将 TKScope 做为日常开发调试以及量产编程的工具。

修订历史

版本	日期	原因
V1.00	2011/12/02	创建文档

销售与服务网络

广州致远电子股份有限公司

地址：广州市天河区车陂路黄洲工业区 7 栋 2 楼
邮编：510660
网址：www.zlg.cn

全国销售与服务电话：400-888-4005

全国服务电话：400-888-4005

销售与服务网络：

广州总公司

广州市天河区车陂路黄洲工业区 7 栋 2 楼
电话：(020)28267985　22644261

北京分公司

北京市海淀区知春路 108 号豪景大厦 A 座 19 层
电话：(010)62536178　62635573

深圳分公司

深圳市福田区深南中路 2072 号电子大厦 12 楼
电话：(0755)83640169　83783155

武汉分公司

武汉市洪山区广埠屯珞瑜路 158 号 12128 室（华中电脑数码市场）
电话：(027)87168497　87168397

成都分公司

成都市一环路南二段 1 号数码科技大厦 403 室
电话：(028)85439836　85432683

上海分公司：上海

上海市北京东路 668 号科技京城东楼 12E 室
电话：(021)53865521　53083451

上海分公司：南京

南京市珠江路 280 号珠江大厦 1501 室
电话：(025)68123923　68123920

上海分公司：杭州

杭州市天目山路 217 号江南电子大厦 502 室
电话：(0571)89719491　89719493

重庆分公司

重庆市九龙坡区石桥铺科园一路二号大西洋国际大厦（赛格电子市场）2705 室
电话：(023)68796438　68797619

西安办事处

西安市长安北路 54 号太平洋大厦 1201 室
电话：(029)87881295　87881296

请您用以上方式联系我们，我们会为您安排样机现场演示，感谢您对我公司产品的关注！