AN12800

i.MX RT10xx针对安全的熔丝设置

第0版 — 2020年3月23日 应用说明

目录

1 简介 1
2 i.MX RT10xx 芯片的安全生命周期 1
3 密钥 2
3.1 超级根密钥哈希 (SRK_HASH) 2
3.2 总线加密引擎密钥选择（BEE_KEY0_SEL 和 BEE_KEY1_SEL） 2
3.3 一次性可编程主密钥 (OTPMK) 2
3.4 软件通用密钥 2 (SW-GP2) 2
3.5 通用 4 (GP4) 2
4 JTAG/调试 3
5 启动配置 3
5.1 BOOT_CFG 3
5.2 BT_FUSE_SEL 3
5.3 DIR_BT_DIS 3
5.4 FORCE_COLD_BOOT 4
6 锁 4
7 安全熔断检查清单 4
8 参考资料 8
9 修订记录 8

1 简介

恩智浦 i.MX RT10xx 系列提供了多种安全特性，其中大部分是利用熔丝控制的。对于安全应用，有一些与安全特性无关的熔丝可能也需要配置。本文档讨论针对安全应用的熔丝设置，并提供熔丝配置的建议。

本应用说明假定您已经熟悉了 i.MX RT10xx 芯片可用的安全特性。有关安全特性的更多信息，请参阅 i.MX RT 芯片的安全参考手册。

2 i.MX RT10xx 芯片的安全生命周期

i.MX RT10xx 芯片的安全生命周期有三个状态：

- 开放（SEC_CONFIG[1]熔丝 = 0）
  - — 用于非安全产品或安全产品的开发阶段。
  - — 签名的镜像文件是可选项。如果提供了签名镜像文件，则执行验签并记录错误（如有），但验签错误不会阻止启动。
  - — SNVS 在启动期间转换到非安全状态。SNVS 主密钥对 DCP 模块不可用。
- 封闭（SEC_CONFIG[1]熔丝 = 1；FIELD_RETURN 熔丝 = 0）：
  - — 用于安全产品。
  - — 签名的镜像文件是强制要求。未经验签的代码无法启动。
  - — SNVS 在启动期间转换到可信状态。只要不发生安全违规（例如连接调试器），DCP 模块便可使用 SNVS 主密钥。
- 现场返修（SEC_CONFIG[1]熔丝 = 1；FIELD_RETURN 熔丝 = 1）：
  - — 用于最终客户退回的安全产品。芯片不应返回服务状态（无法返回“封闭”状态）。
  - — 为了从“封闭”状态变为“现场返修”状态，需要包含 HAB CSF 中的特定命令的签名代码。
    - 使用 HAB CSF 解锁命令，包括设备的唯一 ID（CSF 无法在另一设备上重复使用），现场返修标签位（通常设置为阻止“现场返修”熔丝的编程）可以清零。
    - 使用解锁现场返修命令成功执行 HAB CSF 后，可以将“现场返修”熔丝熔断，允许执行其他调试或将芯片送回恩智浦进行分析。
  - — 签名的镜像文件是可选项。如果提供了签名镜像文件，则执行验签并记录错误（如有），但验签错误不会阻止启动。
  - — 如果未使用 SJC_DISABLE 熔丝将 JTAG 完全禁用，可以重新启用 JTAG（更多信息请参见第 4 节“JTAG/调试”）。

3 密钥

RT10xx 芯片提供了多个密钥和密钥选择熔丝。下文提供关于每个密钥的更详细信息。对于安全应用，SRK_HASH 是唯一必需写入的值。其他的密钥值是可选的，取决于具体应用场景。

3.1 超级根密钥哈希(SRK_HASH)

对于运行验签过的代码的安全应用，必须用一个数值将 SRK_HASH 熔丝熔断。写入熔丝的数值对应于该芯片所用的代码签名密钥对的公开部分。SRK_HASH 用于验证放在签名镜像文件里的公钥表。

注意

SRK_HASH 是从公钥信息生成的，因此不需要对 SRK 实施读取锁定。

3.2 总线加密引擎密钥选择（BEE_KEY0_SEL 和 BEE_KEY1_SEL）

总线加密引擎(BEE)可用于即时解密全部或部分 FlexSPI 存储器。BEE 模块支持两个区域，每个区域可以使用不同的密钥。如果您计划在应用中使用 BEE 模块，必须正确配置 BEE_KEY0_SEL 和 BEE_KEY1_SEL 熔丝，为每个区域选择希望使用的密钥。

即便您不使用加密的“就地执行”(XIP) 启动特性（启动后在软件中配置 BEE 模块），仍然需要配置密钥选择，因为 BEE 模块寄存器中没有用于选择密钥的字段（密钥的选择仅来自熔丝块）。密钥选择的 0b00 选项（默认选项）是“来自寄存器”的选项，允许设置要在 BEE 寄存器中使用的密钥值。但是，必须选择“来自寄存器”熔丝选项才能使用此特性。

除了默认的“来自寄存器”选项，RT10xx 系列产品的可用 BEE 密钥可能不同。有关更多信息，请参阅具体芯片相关的文档。

注意

RT1010 芯片使用 OTFAD 模块而非 BEE。OTFAD 模块具有不同的密钥配置选项，本应用说明不作介绍。

3.3 一次性可编程主密钥 (OTPMK)

OTPMK 是一个因芯片而异（即在每个处理器上都不同）的密钥，用作密钥派生的种子。OTPMK 熔丝值由恩智浦在芯片制造期间写入。该密钥也被锁定，无法直接从熔丝读取。OTPMK 值通过私有总线发送到 SNVS 模块，然后派生出 OTPMK 密钥值，可以将其发送到 DCP 或 BEE 模块使用。OTPMK 派生密钥可以在芯片上使用，但即使恩智浦也无法读取。

3.4 软件通用密钥 2 (SW-GP2)

SW-GP2 熔丝值可以是用户定义的密钥，而非由恩智浦设置的，供 DCP 或 BEE 模块使用。如果 SW-GP2 熔丝用作密钥，建议使用 SW_GP2_LOCK 和 SW_GP2_RLOCK 锁定该熔丝的写入和读取。

3.5 通用 4 (GP4)

在一些 RT10xx 芯片上，GP4 熔丝值可以用作用户定义的密钥，而非由恩智浦设置的，供 BEE 模块使用。如果 GP4 熔丝用作 BEE 密钥，建议使用 GP4_LOCK 锁定该熔丝的写入和读取。

4 JTAG/调试

本芯片提供多种 JTAG 和调试模式，并有多个熔丝来控制其操作。安全应用不应弃调试熔丝于默认状态。有些 MCU 产品在启用“安全”模式时会自动禁用调试，RT10xx 产品与此不同，将芯片置于“封闭”模式对调试功能没有直接影响。封闭的芯片仍可调试，虽然调试会触发 SNVS 模块中的安全违规。

要完全和永久禁用芯片的 JTAG 及调试，请使用以下熔丝设定：

- JTAG_SMODE = 11，设定 JTAG 安全模式为禁止调试
- SJC_DISABLE = 1，禁用 JTAG 模块
- KTE = 1，禁止跟踪
- JTAG_HEO = 1，禁用 JTAG 安全模式下的 HAB 操控

有关在安全模式下使用 JTAG（此时利用挑战/响应机制可以启用调试）的更多信息，请参阅 AN12419，“i.MX RT10xx 的安全 JTAG”。

注意

禁用调试时，即使调试通信处于默认的 SWD 设置，JTAG_TRST 信号也可能会干扰软件复位。在软件复位期间，应将 JTAG_TRST 引脚拉至/驱动为低电平以避免复位发生问题。

5 启动配置

启动配置熔丝并不直接控制安全特性，但它们的使用可能会对整体系统安全性产生影响。以下部分介绍安全系统应如何设置启动配置熔丝。

5.1 BOOT_CFG

芯片的启动配置可以利用 GPIO 操控或熔丝来控制。为了节省引脚并防止攻击者更改启动配置，安全应用应当使用“从熔丝启动”的启动模式(BOOT_MODE[1:0] = 00)。BOOT_CFG 熔丝应针对所使用的特定启动存储器进行相应的配置。恩智浦还建议熔断 BOOT_CFG_LOCK 熔丝，以防止 BOOT_CFG 熔丝在设定完成后被修改。

注意

BOOT_CFG 熔丝区包含除 BOOT_CFG 之外的熔丝，因此 BOOT_CFG_LOCK（和其他熔丝锁）应在所有其他需要的熔丝配置完成之后，作为熔丝配置的最后一步进行设置。

5.2 BT_FUSE_SEL

当使用 BOOT_MODE[1:0] = 00 选项从熔丝启动时，启动流程由 BT_FUSE_SEL 值控制。如果 BT_FUSE_SEL = 0，表示启动设备（例如闪存）尚未编程，启动流程将直接跳转到串行下载器。如果 BT_FUSE_SEL = 1，则遵循正常启动流程，ROM 尝试从所选启动设备启动。因此，为了使用 BOOT_CFG 值进行正常的启动操作，必须熔断 BT_FUSE_SEL。

5.3 DIR_BT_DIS

应当熔断 DIR_BT_DIS 熔丝，以避免使用保留的恩智浦功能。截至本应用说明撰写时，RT106x 芯片在离开恩智浦工厂时，该熔丝已经熔断。未来，对于其他 RT10xx 产品，该熔丝可能在恩智浦制造期间熔断，但目前，您必须规划在安全芯片设置期间熔断该熔丝。

5.4 FORCE_COLD_BOOT

采用 SRC_GPR1[PERSISTENT_ENTRY0]，RT10xx 芯片支持从暂停的低功耗模式快速唤醒的选项。采用此机制时，大部分 ROM 在唤醒期间被旁路，包括代码验签(HAB)。为了提供最高的安全性，恩智浦建议熔断 FORCE_COLD_BOOT 熔丝，以防止使用 PERSISTENT_ENTRY0 段。

6 锁

一般而言，建议在最终安全配置中设置尽可能多的文档中介绍的锁熔丝，以防止恶意或无意的滥用/误用。特别是，应当设置 BOOT_CFG_LOCK 以防止修改启动设置。如上所述，如果使用了任何熔断密钥选项，还建议锁定这些密钥的读取和写入。

7 安全熔断检查清单

下表是针对安全应用的熔丝设定的快速参考。并非所有熔丝都是必需的，但在确定最终熔丝配置时至少应予以审查和考虑。

表 1. 安全熔断检查清单

安全生命周期熔丝				
熔丝	位置	安全应用的 推荐值	锁	备注
SEC_CONFIG[1]	0x460[1]	1	BOOT_CFG_LOCK	对安全产品是必需的。应是由 OEM 设置的最后几个熔丝之一，其后是 BOOT_CFG_LOCK。
FIELD_RETURN	0x400[31]	0	受 OCOTP 控制器中的 标签位保护： FIELD_RETURN_LOCK。	对于安全产品的正常运行，应为 0。可以使用特殊 HAB CSF 命令将现场返修标签位清零，然后可以熔断现场返修熔丝。
密钥和密钥控制熔丝				
熔丝	位置	安全应用的 推荐值	锁	备注
SRK_HASH	0x580[31:0]、 0x590[31:0]、 0x5A0[31:0]、 0x5B0[31:0]、 0x5C0[31:0]、	派生自签名密钥	SRK_LOCK。仅 RT1010 提供写保护和覆盖保护锁。其他 RT10xx 芯片没有 SRK_LOCK。	对安全产品是必需的（用于代码签名验签）。写入熔丝的值对应于芯片所用的代码签名密钥对的公开部分。

表格接下页……

表 1. 安全熔断检查清单（续）

	0x5D0[31:0]、0x5E0[31:0]、0x5F0[31:0]			
SRK_REVOKE[3:0]	0x6F0[3:0]	0	受 OCOTP 控制器中的标签位保护：SRK_REVOKE_LOCK	允许 OEM 通过撤销所选密钥来管理为 HAB 代码签名的根密钥。每一位对应 SRK 表中的一个索引。
BEE_KEY0_SEL	0x460[13:12]	变化量	BOOT_CFG_LOCK	根据需要配置，设置 BEE 区域 0 的密钥。
BEE_KEY1_SEL	0x460[15:14]	变化量	BOOT_CFG_LOCK	根据需要配置，设置 BEE 区域 1 的密钥。
OTPMK	N/A	变化量	N/A	恩智浦设置。由恩智浦编程并锁定的唯一密钥。恩智浦或 OEM 都无法读取 OTPMK。
SW-GP2	0x690[31:0]、0x6A0[31:0]、0x6B0[31:0]、0x6C0[31:0]	变化量	SW_GP2_LOCK 和 SW_GP2_RLOCK	可选的用户设置的密钥。可以用作 DCP 和 BEE 模块的密钥。
GP4	0x8C0[31:0]、0x8D0[31:0]、0x8E0[31:0]、0x8F0[31:0]	变化量	GP4_LOCK 和 GP4_RLOCK	可用作 BEE 密钥，仅 RT106x 提供此选项。
JTAG 和调试熔丝				
熔丝	位置	安全应用的推荐值	锁	备注
JTAG_SMODE	0x460[23:22]	11	BOOT_CFG_LOCK	安全应用应使用 01 模式从而仅启用安全 JTAG，或使用 11 以禁用 JTAG。

表格接下页……

表 1. 安全熔断检查清单（续）

				注：如果 SJC_DISABLE 或 JTAG_HEO 未熔断，可以使用特殊 HAB CSF 重新启用 JTAG。
SJC_DISABLE	0x460[20]	1	BOOT_CFG_LOCK	可以选择性地将 SJC_DISABLE 熔丝熔断，以完全禁用安全 JTAG 控制器。
KTE	0x460[26]	1	BOOT_CFG_LOCK	可以熔断 KTE 熔丝以禁止追踪。如果使用 JTAG_SMODE = 01 或 11 禁用了调试，则还必须熔断 KTE 来禁用调试。
JTAG_HEO	0x460[27]	1	BOOT_CFG_LOCK	可以选择性地将 JTAG_HEO 熔丝熔断，以防止利用 HAB CSF 重新启用调试。
启动配置熔丝				
熔丝	位置	安全应用的推荐值	锁	备注
BOOT_CFG1[7:0]	0x450[7:0]	变化量	BOOT_CFG_LOCK	视需要根据启动配置设置。
BOOT_CFG2[2:0]	0x450[10:8]	变化量	BOOT_CFG_LOCK	视需要根据启动配置设置。
BT_FUSE_SEL	0x460[4]	1	BOOT_CFG_LOCK	熔断 BT_FUSE_SEL 以使用“从熔丝启动”的启动模式。
DIR_BT_DIS	0x460[3]	1	BOOT_CFG_LOCK	置 1 为禁用恩智浦 ROM 测试模式。
FORCE_COLD_BOOT	0x460[5]	1	BOOT_CFG_LOCK	可选择性地置 1，防止利用持久入口字段作为入口点快速唤醒暂停状态（即在暂停唤醒事件中旁路 HAB 重新验签）。

表格接下页……

表 1. 安全熔断检查清单（续）

锁熔丝				
熔丝	位置	安全应用的 推荐值	锁	备注
BOOT_CFG_LOCK	0x400[3:2]	11	N/A	置 1 以防止修改启动配置熔丝。确保在熔断 BOOT_ CFG_LOCK 之前，所有 BOOT_CFG 熔丝（包括 SEC_CONFIG[1]）都已根据需要进行设定。
SW_GP2_LOCK	0x400[21]	1	N/A	可选择性地置 1，防止修改 SW_GP2 密钥。如果使用 SW_GP2 密钥，强烈建议设置此锁。
SW_GP2_RLOCK	0x400[23]	1	N/A	可选择性地置 1，防止软件读取 SW_GP2 密钥。它不会阻止 DCP 和 BEE 模块使用 SW_GP2。
GP4_LOCK	0x400[25:24]	11	N/A	仅限于 RT106x。可选择性地置 1，防止修改 GP4 密钥。如果使用 GP4 密钥，强烈建议设定此锁。
GP4_RLOCK	0x400[7]	1	N/A	仅限于 RT106x。可选择性地置 1，防止软件读取 GP4 密钥。不会阻止 BEE 模块使用 GP4。
其他锁	变化量	变化量	N/A	设置文档中介绍的对于任何你知道的熔丝的锁位，不需要修改该段文字。

8 参考资料

- i.MX RT10xx 安全参考手册（审核下载）
- AN12419，“i.MX RT10xx 的安全 JTAG”
- AN12681，“如何在 i.MX RT10xx 中使用 HAB 安全启动”（审核下载）
- AN12079，“如何使用 i.MXRT 安全启动”（审核下载）

9 修订记录

表 2.：修订记录

修订版本号	日期	重要变化
0	2020 年 3 月	初版

How To Reach

Us Home Page:

nxp.com

Web Support:

nxp.com/support

For more information, please visit: http://www.nxp.com

For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 23 March 2020

Document identifier: AN12800

arm