AN13078
防篡改功能使用指南

Rev. 1 — 11 May, 2021 Application Note

目录

1 简介

本文档介绍了防篡改功能（Tamper Function）的使用。篡改检测可用于保护隐私或敏感信息。当设备遇到未经授权的开启或修改时，将触发防篡改功能把关键信息清空。部分 I.MXRT 系列支持 SNVS 模块的防篡改功能。本指南旨在介绍 i.MXRT1170- EVK 板防篡改功能的使用。

2 概述

该功能支持外部和内部两种防篡改检测。

- 内部提供电压、温度、时钟监控用于防篡改检测。
- 外部采用防篡改引脚检测设备是否遇到未经授权的开启或篡改。

当监测条件参数超出范围时，将触发防篡改功能将关键信息清零，包括 GPR 寄存器、安全 RAM 和可清零主密钥（ZMK），同时将安全状态机（SSM）切换到“失败”状态。

3 防篡改功能介绍

i.MXRT1173 支持内部和外部防篡改检测。

- 十个外部防篡改检测引脚，包括无源和有源篡改检测。
- 三种内部防篡改检测：包括电压、时钟和温度检测。

3.1 外部防篡改检测

外部篡改检测是通过芯片引脚提供特殊机制来决定设备是否遇到了未经授权的打开或篡改。芯片内部将引脚接收到的信号与所期望的信号电平进行比较，一旦不相等，将触发防篡改机制。当使用单个防篡改管脚来检测时，为无源检测；当使用成对的防篡改信号，一个用来发送信号，另外一个用来检测，为有源检测。该芯片最多支持 10 个无源篡改检测引脚，或者 5 对有源篡改检测引脚。

注

如果篡改检测引脚是浮空的并且外部连接很长的走线，这个会带来额外的电流消耗，推荐使能内部的上拉/下拉电阻来避免额外的电流增加。

- 毛刺过滤器

  每个篡改检测引脚都支持启用或不启用毛刺过滤器，并可以通过配置 ETGFx 字段来设置过滤器宽度，脉冲过滤器为宽度 128 ~ 32640 的 SRTC 时钟，启用脉冲滤波器后，外部引脚上任何等于或小于数字脉冲过滤器宽度的信号都会被过滤。图 1 显示了毛刺过滤器工作示例。

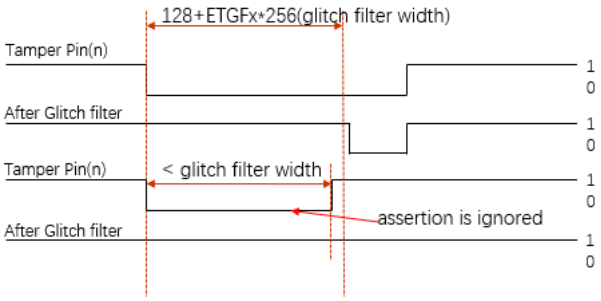

图 1. 脉冲滤波器工作示例

- 无源篡改检测

  每个引脚都支持用于检测与设定电平值是否一致。

  图 2 展示了一个常见的无源篡改检测初始化流程。

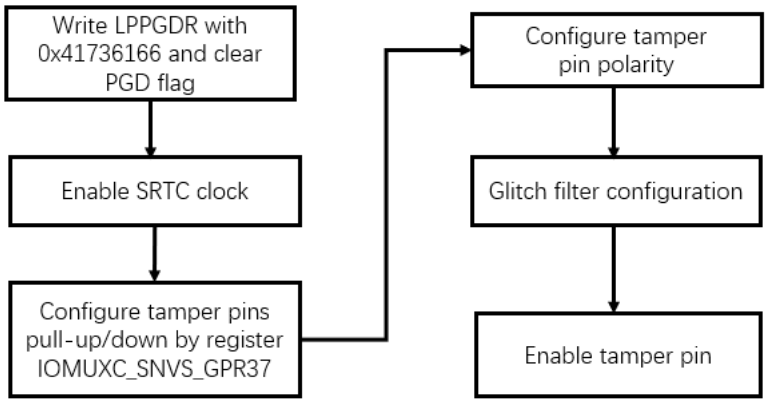

图 2. 无源篡改检测初始化流程图

当检测到引脚电平与寄存器设置的电平不一致时，若已使能防篡改中断，标志位将置位并触发防篡改机制。

- 有源篡改检测

  10 个引脚可用于配置 5 对有源篡改检测。在一对篡改检测引脚中，一个引脚用于输出指定的信号，另一个用于接收信号并检查是否匹配。SNVS_TAMPER9 ~ SNVS_TAMPER5 可用于作为输出引脚，具体关系如下：

  — 有源输出焊盘 5 与检测引脚 9 相连

  — 有源输出焊盘 4 与检测引脚 8 相连

  — 有源输出焊盘 3 与检测引脚 7 相连

  — 有源输出焊盘 2 与检测引脚 6 相连

  — 有源输出焊盘 1 与检测引脚 5 相连

  十个检测引脚都可以作为接收引脚。注意输出和接收不能设置为同一引脚。

  图 3 展示了一个常见的有源篡改检测初始化流程。

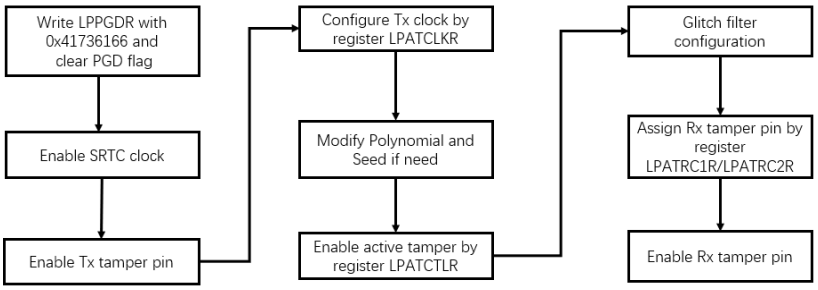

图 3. 有源篡改检测初始化流程图

请将相应的 Tx 和 Rx 引脚连接在一起，当连接断开时，如果中断已使能，将触发防篡改中断。

3.2 内部防篡改检测

温度、电压和时钟的触发条件范围参数在出厂时已预先设置好。如 表 1 所示。

表 1. 预设范围参数

Parameters	Min.	Typ.	Min.	Unit
High Temp Tamper	125	130	135	°C
Low Temp Tamper	-40	-30	-20	°C
Low Temp Tamper (shelf mode)	-60	-50	-40	°C
V_{bat} LVD tamper	2.25	2.325	2.4	V
V_{bat} HVD tamper	4.25	4.375	4.5	V
Regulator LVD Tamper	1.48	1.58	1.68	V
Regulator HVD tamper	1.86	1.96	2.06	V
Clock low freq. tamper	15	20	25	kHz
Clock high freq. tamper	40	52.5	80	kHz

也可以通过配置寄存器 IOMUXC_SNVS_GPR_GPR35 来调整触发条件范围，详情请参考 *i.MX RT1170 Processor Reference Manual* (document IMXRT1170RM).

- 电压检测

  SNVS 模拟 IP 提供 VBAT 电源监控和 VREG 电源监控功能。如果其中任意一个的电源电压超过了相应的电压范围，该模块将置位相应的标志位表示检测到电压篡改事件。

  电压检测默认为禁用状态，需要在寄存器 LPTDCR 中配置 VT_EN 位字段来使能电压检测功能。检测值小于 2.25 V 或大于 4.5 V 的 Vbat 电压，或小于 1.48 V 或大于 2.06 V 的 SNVS 稳压器输出电压（VDD_SNVS_ANA）将设置标志并产生中断表示检测到电压篡改事件。

- 时钟频率检测

  时钟频率检测包括两个子检测模块：non-clk 检测模块和时钟检测模块。non-clk 检测器负责监测 osc32k 是否停止振荡，时钟检测器负责监测时钟频率是否超出范围。当检测到 osc32k 异常时，该模块将使能 irc32k 作为输出时钟，同时置位相应的标志表示检测到时钟篡改事件。

  时钟检测功能默认为禁用状态，需要在寄存器 LPTDCR 中配置 CT_EN 位字段来使能时钟频率检测功能，检测值小于 15 KHz 或大于 80 KHz 的时钟频率将设置标志并产生中断表示检测到时钟频率篡改事件。

- 温度检测

温度检测功能用于监视当前温度是否超出范围。当检测到温度异常时，该模块将置位相应的标志位表示检测到温度篡改事件。

温度检测功能默认为禁用状态，需要将寄存器 LPTDCR 中配置 TT_EN 位字段来使能温度篡改检测功能。检测值低于-60 °C（shelf mode）或高于 135 °C 时将设置标志并产生中断表示检测到温度篡改事件。

4 例程

AN13078SW 可供在 MIMXRT1170-EVK 板上运行，以测试防篡改功能，i.MXRT1170 EVK 板如 图 4 所示。

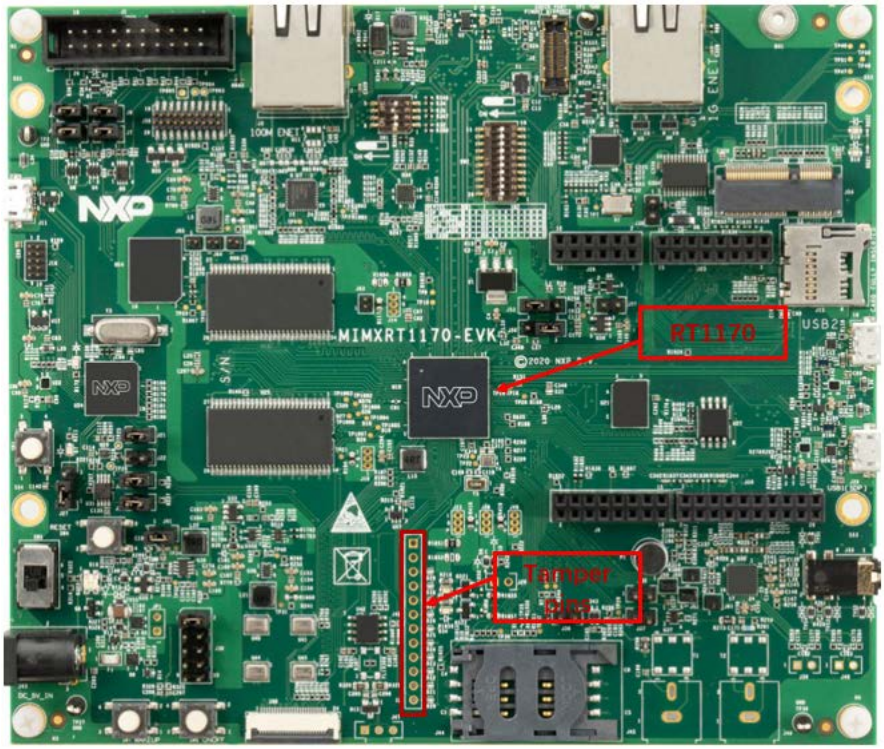

图 4. i.MXRT1170 EVK 板

1. 解压 AN13078SW，并下载到 i.MXRT1170 EVK 板。
2. 运行所附例程时，系统将打印输出如 图 5 所示信息。

```
SNVS tamper test
1 - passive tamper pin
2 - active tamper pin
3 - voltage tamper test
4 - temperature tamper test
5 - clock tamper test

Waiting for tamper test select...
```

图 5. 运行例程后系统打印输出的信息

3. 输入 1-5 选择所需测试。

4.1 外部防篡改检测

外部防篡改检测包括无源检测和有源检测，输入“ 1”选择无源篡改检测，输入“ 2”选择有源篡改检测。

- 无源篡改检测

  请按照以下步骤测试无源篡改检测。

  1. 输入“ 1”选择无源篡改检测。
  2. 按照指示信息输入测试引脚编号（0-9），输入前，请保证相应的引脚保持低电平，否则将设置标志位表示检测到篡改事件。
  3. 例如，输入“ 1”，如果不将引脚 2 连接到 GND，系统将会输出如 图 6 所示信息。

```
Waiting for tamper pins input(0~9)...


if tamper pin 2 is not low level, will trigger tamper violation
External Tampering 2 Detected
ZMK is cleared

press any key to exit ...
```

图 6. 无源篡改检测

  在此示例中，引脚 2 检测到篡改事件并清除了 ZMK。

  4. 按照上述步骤将检测脚拉至高电平或低电平，通过打印消息检查结果。

- 有源篡改检测

  请按照以下步骤测试有源篡改检测。

  1. 输入“ 2”选择有源篡改检测。
  2. 按照指示信息输入 Tx 和 Rx 检测引脚，请注意将相应的 TX 和 RX 引脚连接在一起，否则将设置标志并产生中断表示检测到篡改事件。
  3. 例如，在 Tx 引脚选择输入“ 8”，Rx 引脚选择输入“1”。输出信息如 图 7 所示。

```
Waiting for tamper tx pins input(5~9)...

Waiting for tamper rx pins input(0~9)...

if tamper pin tx 9 and rx pin 2 don't connect together, will trigger tamp
er violation
No External Tampering Detected
ZMK is not zero!

press any key to exit ...
```

图 7. 有源篡改检测

  4. 按照上述步骤将输入输出引脚连接或者断开，并通过打印消息检查结果。

4.2 电压检测

1. 给 SNVS 电源提供 3.0 V 电压，拆下 R419，通过 J28 的引脚 3 为 SNVS 供电，打开系统电源。
2. 输入“ 3”选择电压检测。
3. 输入“ 1”使能电压检测。
4. 关闭系统电源，保持 SNVS 电源打开，并以小步长增加/降低电压。

5. 接通系统电源，输入“ 3”以选择电压检测。
6. 输入“ 2”查看电压测试结果。

系统将输出测试结果。

4.3 时钟检测

1. 通过可调时钟源来替代 32Khz 晶体时钟，卸下 i.MXRT1170 EVK 板上的 Y5。
2. 打开 i.MXRT1170 EVK 板的电源。
3. 输入“ 5”选择时钟检测。
4. 输入“ 1”使能时钟检测。
5. 逐步增加/减少时钟频率。
6. 根据指示信息输入“ 5”选择时钟检测。
7. 输入“ 2”查看时钟测试结果。

系统将输出测试结果。

4.4 温度检测

1. 打开 i.MXRT1170 EVK 板的电源。
2. 输入 "4 "选择温度检测。
3. 输入 "1 "使能温度检测器。
4. 升高/降低 i.MXRT1170 的环境温度。
5. 根据指示信息输入 "4"，选择温度检测。
6. 输入 "2 "查看温度测试结果。

系统将输出测试结果。

5 参考资料

- *Security Reference Manual for the i.MX RT1170 Processor* (document IMXRT1170SRM)
- *i.MX RT1170 Processor Reference Manual* (document IMXRT1170RM).
- *i.MX RT1170 Crossover Processors Data Sheet for Industrial Products* (document IMXRT1170IEC)

6 版本历史

版本号	日期	重大更新
0	7 December, 2020	首次发布
1	11 May, 2021	• 外部防篡改检测中增加一注释 • 更新 图 5 • 更新 图 7

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: 11 May, 2021

Document identifier: AN13078

arm