AN13078

How to Use Tamper Function

Rev. 1 — 11 May, 2021 Application Note

Contents

1 Introduction

Tamper detection is a special mechanism to trigger violation and zeroize key information when the device encounters unauthorized opening or tampering, which can be use to protect the sensitive data against leakage or others. Some i.MX RT series support tamper function by SNVS modules. This application note intends to introduce how to use tamper function on i.MXRT1170-EVK board.

2 Overview

There are two types of tamper detection supported, external and internal.

- The internal tamper detection supports voltage, temperature, and clock monitors.
- The external tamper detection takes external tamper pins to detect whether the device encounters unauthorized opening or tampering.

When monitoring conditions are out of range, it will trigger violation and take action to zeroize key information, including GPR register, security RAM and Zeroizable Master Key (ZMK), as well as Secure State Machine (SSM) transition to fail state.

3 TAMPER introduction

Internal and external tamper are supported on i.MXRT1173.

- Ten external tamper pins, including passive and active tampers
- Three internal tamper functions: voltage, clock and temperature tamper

3.1 External tamper pins

External tamper detection is a special mechanism provided through a chip pin to detect whether the device encounters unauthorized opening or tampering. Inside the chip, the received signal is compared with the desired signal level. Once unequal, tamper event is triggered. When the desired signal is fixed, it is a passive tamper; when the desired signal level is also toggling with time, it is an active tamper. The chip supports at most ten passive tamper detection pins, or five active tamper pairs alternatively.

NOTE

If tamper pins are floating and connect the long trace externally, it possibly cause extra current consumption. Recommend to enable internal pull-up/down resistor to avoid extra current adder.

- Glitch filter

  Each tamper pin can support to enable glitch filter or not, also can configure ETGFx bit field to set filter width, glitch filter width is from 128 to 32640 SRTC clock, after enable glitch filter, any assertion on external tamper pin that is equal to or less than the value of the digital glitch filter is ignored. Figure 1 shows the glitch filter functions introduced.

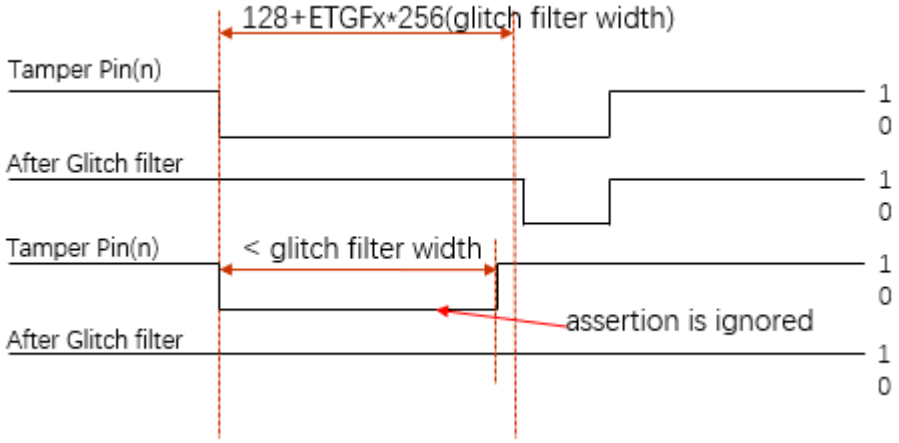

Figure 1. Glitch filter working

- Passive tamper

  Each tamper pin can be used to detect if it matches the expected status.

  Figure 2 shows a common initialization flow.

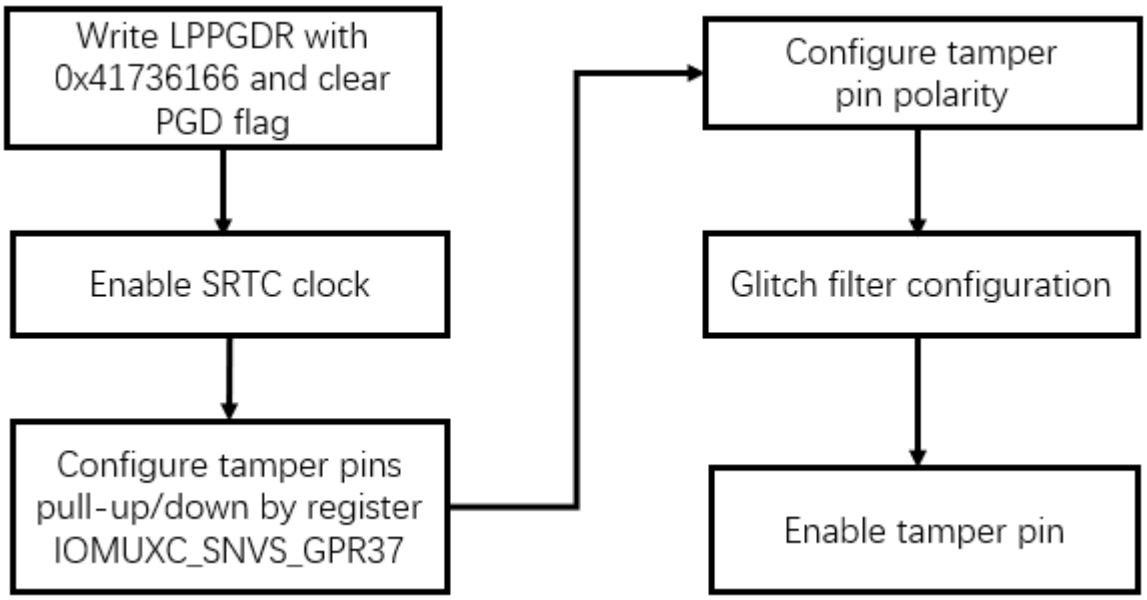

Figure 2. Passive tamper initialization flow

When detecting the tamper level does not match the tamper polarity set by registers, it will set corresponding tamper flag and trigger violation. Also, it may enable tamper interrupt.

- Active tamper

  Ten tamper pins are available to be configured to get five pairs of active tamper. In one pair, one tamper is used to output specified signal and the other to receive signal and check whether it matches or not.

  `SNVS_TAMPER1` - `SNVS_TAMPER5` can be used to Tx pads. The relation is as below:

  — Active Tamper 5 Tx pad is hardware fixed to Tamper pin 9

  — Active Tamper 4 Tx pad is hardware fixed to Tamper pin 8

— Active Tamper 3 Tx pad is hardware fixed to Tamper pin 7

— Active Tamper 2 Tx pad is hardware fixed to Tamper pin 6

— Active Tamper 1 Tx pad is hardware fixed to Tamper pin 5

All ten tamper pins can be used on Rx pad. The Tx and Rx pad should not be a same pin.

Figure 3 shows a common initialization flow.

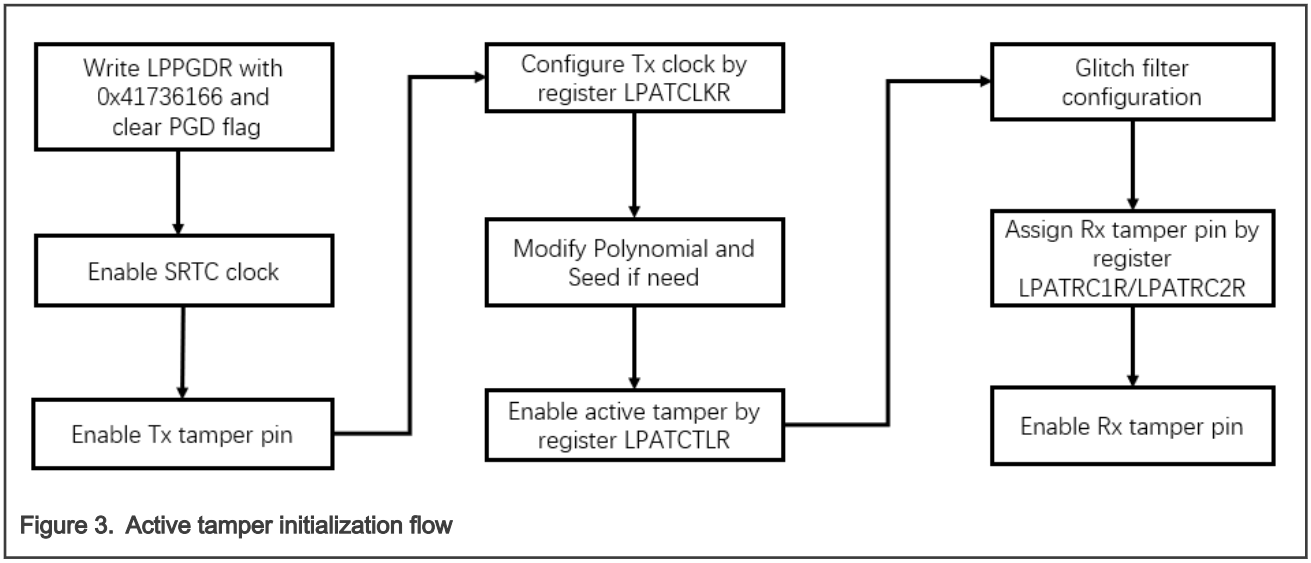

Figure 3. Active tamper initialization flow

Please connect corresponding Tx and Rx pins together. When the connection is OFF, it will trigger violation and generate tamper interrupt if interrupt is enabled.

3.2 Internal tamper

Temperature, voltage and clock tamper range are trimmed in factory. Table 1 describes the trimmed tamper range.

Table 1. Trimmed tamper range

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

Also may adjust detection offset by register, `IOMUXC_SNVS_GPR_GPR35`. For details, see *i.MX RT1170 Processor Reference Manual* (document IMXRT1170RM).

- Voltage detectors

SNVS analog IP provides VBAT power supply monitor and VREG power supply monitor functions. If any of those involved voltages exceeds the appropriate voltage range of their own, this module will set the corresponding flag, indicating that a voltage tamper happens.

By default, voltage detector is disable, need to set `VT_EN` bit field in register LPTDCR to enable voltage tamper. When Vbat voltage is less than 2.25 V or greater than 4.5 V, or when SNVS regulator output voltage, `VDD_SNVS_ANA`, is less than 1.48 V or greater than 2.06 V, voltage tamper will be asserted.

- Clock frequency detector

  The clock frequency detector actually includes two sub detectors: non-clk detector and clock detector. Non-clk detector will monitor whether osc32k stopped oscillating and clock detector will monitor whether the frequency is out of range. When osc32k is detected abnormal, this module will enable irc32k to act as output clock and meanwhile set the corresponding flag to indicate clock tampering detected.

  By default, clock detector is disable, need to set CT_EN bit field in register LPTDCR to enable clock tamper. It will assert clock tamper when clock frequency is less than 15 KHz or greater than 80 KHz.

- Temperature detector

  The Temperature detector function is to monitor whether the current temperature is out of range. When the temperature is detected abnormal, this module will set the corresponding flag to indicate temperature tampering detected.

  By default, temperature detector is disable, need to set TT_EN bit field in register LPTDCR to enable temperature tamper. It will assert temperature tamper when temperature is less than -60 °C (shelf mode) or greater than 135 °C.

4 Demos

AN13078SW can run on MIMXRT1170-EVK board to show the tamper function. Figure 4 shows the i.MXRT1170 EVK board.

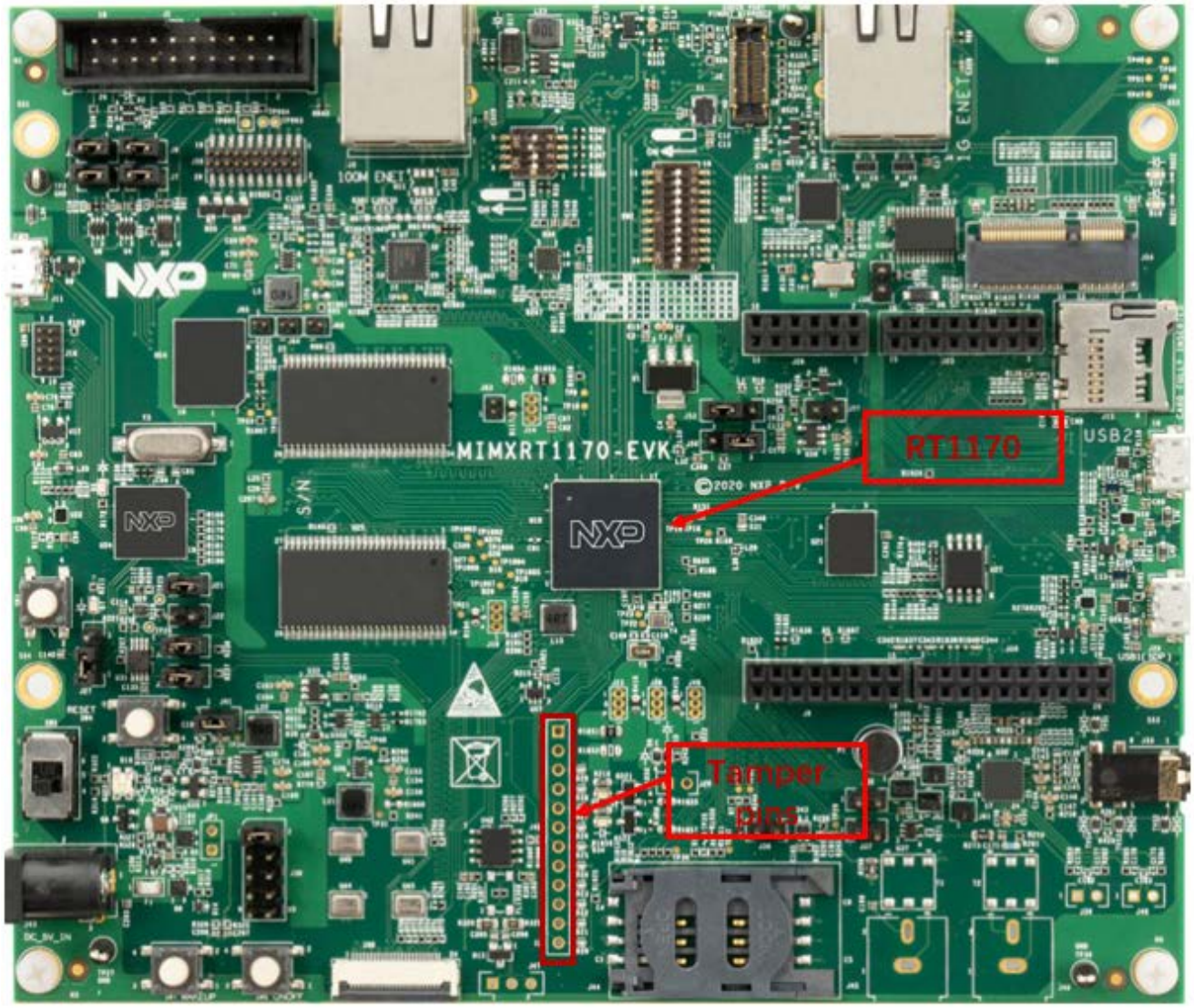

Figure 4. i.MXRT1170 EVK board

1. Unzip AN13078SW and download it to the i.MXRT1170 EVK board.
2. The message, as shown in Figure 5, is printed on running the attached firmware.

```
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...
```

Figure 5. Print message on running demo code

3. Input 1-5 to select the test what you want.

4.1 External pin tamper

Pin tamper contains passive tamper and active tamper test. Input **1** for passive tamper or **2** for active tamper.

- Passive tamper

  Follow steps below to test passive tamper:

  1. Input **1** to select passive tamper test.
  2. Follow the indication message to input tamper number, 0-9. Before input, keep the corresponding tamper pin to low level. Otherwise, tamper will be detected.
  3. For example, input **1**, and if tamper 2 is not connected to GND, the printed message is as shown in Figure 6.

```
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 ...
```

Figure 6. Passive tamper test

  In this example, tamper 2 is triggered and ZMK is cleared.

  4. Follow above steps to drive tamper pin to high or low. Check result by print message.

- Active tamper

  Follow steps below to test active tamper:

  1. Input **2** to select active tamper test.
  2. Follow the indication message to input Tx and Rx tamper pins. Be sure to connect the corresponding TX and RX pin together. Otherwise, tamper will be detected.
  3. For example, input **8** for TX and **1** for RX. The printed message is as shown in Figure 7.

```
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 ...
```

Figure 7. Active tamper test

  4. Follow above steps to disconnect tamper pins or not. Check result by print message.

4.2 Voltage tamper

1. Connect 3.0 V power supply to SNVS power, remove R419, and power to SNVS by pin3 of J28, switch on the system.
2. Input **3** to select voltage tamper test.

3. Input **1** to enable **voltage tamper**.
4. Switch off the system, keep SNVS ON, and increase/decrease the voltage in small step.
5. Switch on the system, input **3** to select voltage tamper test.
6. Input **2** to check **voltage tamper**.

The result will be printed.

4.3 Clock tamper

1. Input 32 Khz clock by adjustable clock source instead of crystal mounted in board. Remove Y5 from the i.MXRT1170 EVK board.
2. Power on the i.MXRT1170 EVK board.
3. Input **5** to select clock tamper test.
4. Input **1** to enable **clock tamper**.
5. Increase/decrease the clock in small step.
6. Input **5** to select clock tamper test following indicated information.
7. Input **2** to check **clock tamper**.

The result will be printed.

4.4 Temperature tamper

1. Power on the i.MXRT1170 EVK board.
2. Input **4** to select temperature tamper test.
3. Input **1** to enable **temperature tamper**.
4. Increase/decrease the temperature of i.MXRT1170.
5. Input **4** to select temperature tamper test following indicated information.
6. Input **2** to check **temperature tamper**.

The result will be printed.

5 Reference

- *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 Revision history

Rev.	Date	Substantive changes
0	7 December, 2020	Initial release
1	11 May, 2021	• Add a note in External tamper pins • Updated Figure 5 • Updated Figure 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