MT793X IoT SDK for GCPU

User Guide

Version: 0.1

Release date: 2021-04-05

Version History

Version	Date	Description
0.1	2021-04-05	Initial draft

Table of Contents

List of Figures

List of Tables

1 Overview

This document describes basic concepts of the GCPU (General Copy Protection Unit), especially in the aspect of software.

2 Instruction

2.1 What Is GCPU

The General Copy Protection Unit (GCPU) is a micro-processor based module. The main function of this module is to provide various copy protection algorithms, such as CPPM, CPRM, AES/AES-CMAC/AES-XCBC-MAC, DES, SHA-1/SHA-224/SHA-256, MD5, RSA, and TRNG.

The GCPU mainly communicates through the APB bus and the AXI bus. The encrypted bit stream can be fed to the the GCPU through the AXI bus. Then, the command and mode can be issued through the APB bus. The decrypted bit stream is stored back to the DRAM through the AXI bus and fetched by other modules.

The GCPU also provides the interface to the eFuse and the ECC module. It generates proper I/O signals to the eFuse and reads the eFuse bits. The GCPU also uses the TX/RX bus to access the ECC module.

2.2 Architecture Diagram

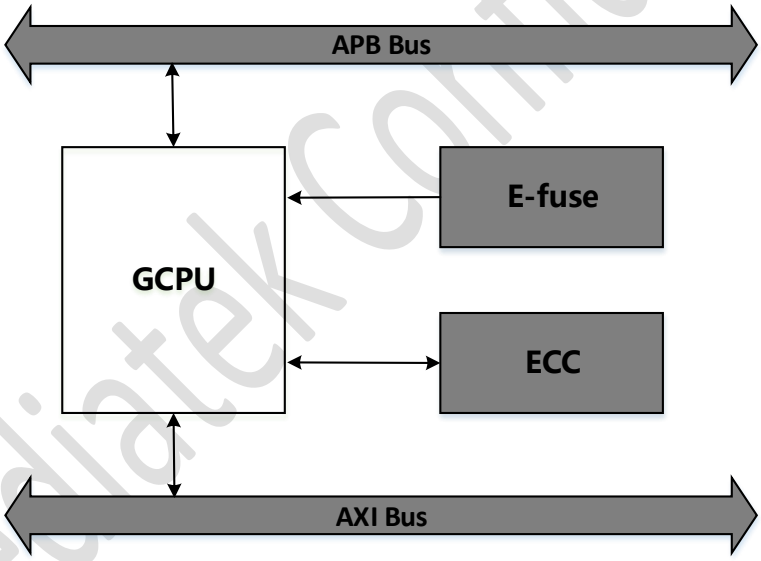

Figure 1. GCPU Architecture Diagram

3 Feature

- 64 x 128 bits internal Data SRAM(DMEM) for access
- 128 x 88 bits internal Instruction SRAM(IMEM) for spare usage
- 8K x 22 bits internal Instruction ROM(IROM) for storing micro codes
- CPPM/CPRM related functions
- AES
- DES
- SHA-1/SHA-224/SHA-256
- MD5
- RSA
- Internal TRNG
- Interaction with ECC
- eFuse reading

4 Programming Guide

4.1 Driver Code List

- Driver/chip/mt7933/src/hal_aes.c
- Driver/chip/mt7933/src/hal_des.c
- Driver/chip/mt7933/src/hal_md5.c
- Driver/chip/inc/ hal_aes.h
- Driver/chip/inc/ hal_des.h
- Driver/chip/inc/ hal_md5.h

4.2 GDMA API List

NUM	API list (hal_des)
1	Hal_aes_cbc_encrypt()
2	Hal_aes_cbc_decrypt()
3	Hal_aes_ecb_encrypt()
4	Hal_aes_ecb_decrypt()
5	Hal_aes_cmac_subkey()
6	Hal_aes_cmac_message()
7	Hal_aes_gcm_encrypt()
8	Hal_aes_gcm_decrypt()

Table 1. DES API List

NUM	API list (hal_aes)
1	Hal_des_cbc_encrypt()
2	Hal_des_cbc_decrypt()
3	Hal_des_ecb_encrypt()
4	Hal_des_ecb_decrypt()

Table 2. AES API List

NUM	APIs list (hal_md5)
1	Hal_md5_init()
2	Hal_md5_append()
3	Hal_md5_end()

Table 3. MD5 API List

4.3 Programming Sequence

- AES GCM
  (1) Set message source DRAM address
  (2) Set encrypted message destination DRAM address
  (3) Set initial source DRAM address
  (4) Set additional authentication source DRAM address
  (5) Set message transfer length (in unit of bits)
  (6) Set initial source transfer length (in unit of bits)
  (7) Set additional authentication transfer length (in unit of bits)
  (8) Call gcpu_exe_cmd with cmd EGCM/DGCM.

- AES CBC
  (1) Set source DRAM address
  (2) Set destination DRAM address
  (3) Set data transfer length (in unit of 128 bits)
  (4) Set key length
  (5) Set key value
  (6) Set initialization vector
  (7) Call gcpu_exe_cmd with cmd ECBC/DCBC.

- AEC ECB
  (1) Set key length
  (2) Set data value
  (3) Set key value
  (4) Call gcpu_exe_cmd with cmd EPAK/DPAK.

- DES CBC
  (1) Set source DRAM address
  (2) Set destination DRAM address
  (3) Set packet number
  (4) Set key value
  (5) Set key length

(6) Set initialization vector

(7) Call gcpu_exe_cmd with cmd TDES_CBC_E/ TDES_CBC_D.

- DES ECB

(1) Set source DRAM address

(2) Set destination DRAM address

(3) Set packet number

(4) Set key value

(5) Set key length

(6) Call gcpu_exe_cmd with cmd TDES_DMA_E/ TDES_DMA_D.

4.4 Configuration

- Path:

project\<borad>\apps\<application>\inc\ hal_feature_config.h

HAL_AES_MODULE_ENABLED

HAL_DES_MODULE_ENABLED

HAL_MD5_MODULE_ENABLED

Exhibit 1 Terms and Conditions

Your access to and use of this document and the information contained herein (collectively this "Document") is subject to your (including the corporation or other legal entity you represent, collectively "You") acceptance of the terms and conditions set forth below ("T&C"). By using, accessing or downloading this Document, You are accepting the T&C and agree to be bound by the T&C. If You don't agree to the T&C, You may not use this Document and shall immediately destroy any copy thereof.

This Document contains information that is confidential and proprietary to MediaTek Inc. and/or its affiliates (collectively "MediaTek") or its licensors and is provided solely for Your internal use with MediaTek's chipset(s) described in this Document and shall not be used for any other purposes (including but not limited to identifying or providing evidence to support any potential patent infringement claim against MediaTek or any of MediaTek's suppliers and/or direct or indirect customers). Unauthorized use or disclosure of the information contained herein is prohibited. You agree to indemnify MediaTek for any loss or damages suffered by MediaTek for Your unauthorized use or disclosure of this Document, in whole or in part.

MediaTek and its licensors retain titles and all ownership rights in and to this Document and no license (express or implied, by estoppels or otherwise) to any intellectual propriety rights is granted hereunder. This Document is subject to change without further notification. MediaTek does not assume any responsibility arising out of or in connection with any use of, or reliance on, this Document, and specifically disclaims any and all liability, including, without limitation, consequential or incidental damages.

THIS DOCUMENT AND ANY OTHER MATERIALS OR TECHNICAL SUPPORT PROVIDED BY MEDIATEK IN CONNECTION WITH THIS DOCUMENT, IF ANY, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. MEDIATEK SPECIFICALLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, COMPLETENESS OR ACCURACY AND ALL WARRANTIES ARISING OUT OF TRADE USAGE OR OUT OF A COURSE OF DEALING OR COURSE OF PERFORMANCE. MEDIATEK SHALL NOT BE RESPONSIBLE FOR ANY MEDIATEK DELIVERABLES MADE TO MEET YOUR SPECIFICATIONS OR TO CONFORM TO A PARTICULAR STANDARD OR OPEN FORUM.

Without limiting the generality of the foregoing, MediaTek makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does MediaTek assume any liability arising out of the application or use of any product, circuit or software. You agree that You are solely responsible for the designing, validating and testing Your product incorporating MediaTek's product and ensure such product meets applicable standards and any safety, security or other requirements.

The above T&C and all acts in connection with the T&C or this Document shall be governed, construed and interpreted in accordance with the laws of Taiwan, without giving effect to the principles of conflicts of law.