# 32-bit RISC Microcontroller
# Reference Manual

# Security Function (SECG2-A)

## Revision 1.0

**2026-01**

Toshiba Electronic Devices & Storage Corporation

# Contents

Preface ..... 3
Related Document ..... 3
Conventions ..... 4
1. Outlines ..... 6
2. Configuration ..... 6
3. Function and Operation ..... 7
3.1. Chip Protect (CPRO) ..... 7
3.1.1. Function ..... 7
3.1.2. Operation ..... 7
3.2. Secure Access Memory (SAM) ..... 9
3.2.1. Function ..... 9
3.3. Non-releasable Flash Protect (NRFP) ..... 10
3.3.1. Function ..... 10
3.3.2. Operation ..... 10
3.4. TOSHIBA Test Mode Control (TCON) ..... 10
3.4.1. Function ..... 10
3.4.2. Operation ..... 10
3.5. RAM Transfer Command (Single Boot Mode) ..... 11
3.5.1. Function ..... 11
3.5.2. Operation ..... 11
4. Example of Usage ..... 12
5. Revision History ..... 14
RESTRICTIONS ON PRODUCT USE ..... 15

# List of Figures

Figure 2.1 Security Function ..... 6

# List of Tables

Table 3.1 Targets of Chip Protect ..... 7
Table 5.1 Revision History ..... 14

# Preface

## Related Document

| 文書名 |
| --- |
| Datasheet |
| Clock Control and Operation Mode |
| Exception |
| Secure Access Memory |
| Flash Memory |

### Conventions

- Numeric formats follow the rules as shown below:
  Hexadecimal: 0xABC
  Decimal: 123 or 0d123 - Only when it needs to be explicitly shown that they are decimal numbers.
  Binary: 0b111 - It is possible to omit the "0b" when the number of bits can be distinctly understood from a sentence.
- "_N" is added to the end of signal names to indicate low active signals.
- It is called "assert" that a signal moves to its active level, "deassert" to its inactive level.
- When two or more signal names are referred, they are described like as [m:n].
  Example: S[3:0] shows four signal names S3, S2, S1 and S0 together.
- The characters surrounded by ***[ ]*** defines the register.
  Example: ***[ABCD]***
- "N" substitutes suffix number of two or more same kind of registers, fields, and bit names.
  Example: ***[XYZ1]***, ***[XYZ2]***, ***[XYZ3]*** → ***[XYZn]***
- "x" substitutes suffix number or character of units and channels in the register list.
- In case of unit, "x" means A, B, and C, ...
  Example: ***[ADACR0]***, ***[ADBCR0]***, ***[ADCCR0]*** → ***[ADxCR0]***
- In case of channel, "x" means 0, 1, and 2, ...
  Example: ***[T32A0RUNA]***, ***[T32A1RUNA]***, ***[T32A2RUNA]*** → ***[T32AxRUNA]***
- The bit range of a register is written like as [m: n].
  Example: Bit[3: 0] expresses the range of bit 3 to 0.
- The configuration value of a register is expressed by either the hexadecimal number or the binary number.
  Example: ***[ABCD]***<EFG> = 0x01 (hexadecimal), ***[XYZn]***<VW> = 1 (binary)
- Word and byte represent the following bit length.
  Byte: 8 bits
  Half word: 16 bits
  Word: 32 bits
  Double word: 64 bits
- Properties of each bit in a register are expressed as follows:
  R:Read only
  W: Write only
  R/W: Read and write are possible.
- Unless otherwise specified, register access supports only word access.
- The register defined as "Reserved" must not be rewritten. Moreover, do not use the read value.
- The value read from the bit having default value of "-" is unknown.
- When a register containing both of writable bits and read-only bits is written, read-only bits should be written with their default value, In the cases that default is "-", follow the definition of each register.
- Reserved bits of the write-only register should be written with their default value. In the cases that default is "-", follow the definition of each register.
- Do not use read-modified-write processing to the register of a definition which is different by writing and read out.

# 1. Outlines

The product has security functions designed to protect internal data, product controls, and other assets.

| Function classification | Function | Operation explanation |
|---|---|---|
| Communication blocking | Chip Protect (CPRO) | Prohibits or restricts the following functions:<br>- Debug tool (JTAG/SW)<br>- RAM monitor tool (NBDIF)<br>- Flash writer tool (in the Flash Writer Mode) |
| Memory access control | Secure Access Memory (SAM) | Controls access from the bus master to memory.<br>SAM has three states, and the accessible areas are defined for each state.<br>Prohibits the Single Boot Mode. |
| Flash memory write/erase prohibition | Non-releasable Flash Protect (NRFP) | Prohibits erase/write of the Flash memory.<br>Once enabled, it cannot be released.<br>Prohibits the Single Boot Mode and Flash Writer Mode. |
| Test mode control | TOSHIBA Test Mode Control (TCON) | Prohibits transition to TOSHIBA test mode.<br>Prohibits the Flash Writer Mode. |
| Password authentification | Single Boot Mode<br>RAM Transfer command | Password authentication with a data length of 255 bytes is required to execute RAM Transfer commands in Single Boot Mode. |

# 2. Configuration

Figure 2.1 outlines the relationship between the functions in the product and the security functions. The dotted box represents the protection provided by the security functions.

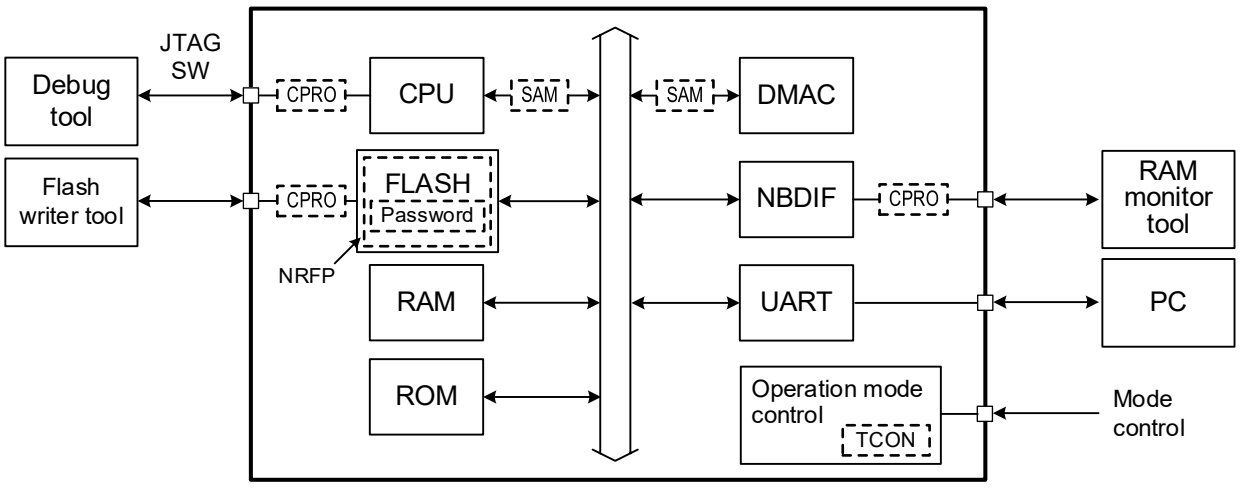


**Figure 2.1 Security Function**

# 3. Function and Operation

Refer to the reference manual "Flash Memory" for the Flash commands and the registers described in this chapter.

## 3.1. Chip Protect (CPRO)

### 3.1.1. Function

The Chip Protect prohibits or restricts the functions of a debug tool and a flash writer tool.

Table 3.1 shows the targets of the Chip Protect.

**Table 3.1 Targets of Chip Protect**

| Target | Function |
|---|---|
| Debug tool | Blocks communication via JTAG or serial wire (SW) |
| RAM monitor tool | Blocks communication via NBDIF pins |
| Flash writer tool | Prohibits reading and writing the Flash memory in the Flash Writer Mode<br>The Flash Writer Mode does not start when the Secure Access Memory is enabled. |

The Flash Writer Mode specifications are not disclosed.

Some products do not have the Non break debugging interface. Confirm the built-in functions of the product in the "Datasheet".

### 3.1.2. Operation

The Chip Protect consists of the Chip Protect bit and the Chip Protect Mask Register ***[FCCPROMR]***. The Chip Protect is enabled when both the Chip Protect bit and the Chip Protect Mask Register are set to "1". The Chip Protect status is checked by the Chip Protect/TOSHIBA Test Mode Control Status Register ***[FCCPROTCONSR]*** <CPROSTA>.

#### 3.1.2.1. Chip Protect Bit

The Chip Protect bit is a nonvolatile bit in the Flash memory and cannot be accessed directly. The Chip Protect bit is operated by Flash commands.

To enable the Chip Protect, the Chip Protect bit must be set to "1". The Chip Protect bit is set to "0" at the time of shipment.

#### 3.1.2.2. Chip Protect Mask Register (*[FCCPROMR]*)

***[FCCPROMR]***<CPROMSK> can temporarily mask (disable) the Chip Protect bit. "1" is the unmasked state and "0" is the masked state.

To rewrite ***[FCCPROMR]***<CPROMSK>, follow the steps below.

(1) Write "0xA74A9D23" to ***[FCKCR]***.
(2) After (1), write to ***[FCCPROMR]***<CPROMSK> within 16 clocks.

***[FCCPROMR]***<CPROMSK> is initialized only by POR and PORF. The value after initialization is "1".

### 3.1.2.3. Temporary Release of Chip Protect

By changing the setting of ***[FCCPROMR]***<CPROMSK>, the Chip Protect can be temporarily released.

If ***[FCCPROMR]***<CPROMSK> is set to "0" while the Chip Protect is enabled, the Chip Protect is released.

Note: If the Secure Access Memory is enabled, writing to ***[FCCPROMR]***<CPROMSK> is not possible in App state.

### 3.1.2.4. Operation of Chip Protect Bit

To set the Chip Protect bit to "1", execute the Automatic CPRO Programming command.

To clear the Chip Protect bit to "0", execute the Automatic CPROTCON Releasing command.

When executing the Automatic CPROTCON Releasing command, the behavior varies depending on the value of ***[FCCPROMR]***<CPROMSK>.

(1) When ***[FCCPROMR]***<CPROMSK> is "0" (Chip Protect temporarily released)

The Chip Protect bit is set to "0" and TOSHIBA Test Mode Control is disabled.

(2) When ***[FCCPROMR]***<CPROMSK> is "1" (Chip Protect enabled)

After all data in the Flash memory is erased, the Chip Protect bit is set to "0" and TOSHIBA Test Mode Control is disabled.

However, if the Non-releasable Flash Protect is enabled, the Automatic CPROTCON Releasing command is ignored.

The value of the Chip Protect bit does not reflect the change until a reset occurs after executing the Automatic CPRO Programming or the Automatic CPROTCON Releasing command.

## 3.2. Secure Access Memory (SAM)

Here is an overview of the Secure Access Memory. For details, refer to the reference manual "Secure Access Memory."

When using the Secure Access Memory, it is recommended to also enable the Chip Protect to block illegal access from outside.

### 3.2.1. Function

The Secure Access Memory controls the access of the Flash memory and RAM from bus masters. It has the following three states, with each state specifying accessible areas.

- Boot state
  A state in which the startup program operates.
- App state
  A state in which the application program operates.
- Lib state
  A state in which the program is operating in isolation from the application program.

Accessing an area not allowed in each state will cause a SAM reset.

NMIs during Boot and Lib states are treated as SAM resets.

Writing to ***[FCCPROMR]*** is not possible in App state.

The Automatic SAMNRFP Releasing command is disabled by the Lock Setting of the Automatic SAMNRFP Programming command. This makes it impossible to disable the Secure Access Memory and Non-releasable Flash Protect.

The following mode does not start when the Secure Access Memory is enabled:

- Single Boot Mode

## 3.3. Non-releasable Flash Protect (NRFP)

### 3.3.1. Function

The Non-releasable Flash Protect prohibits write/erase of the specified Flash memory area. Unlike the Flash Protect (FPRO), the lock Setting prevents it from being released. However, it can be released in our test mode for failure analysis. (When The TOSHIBA Test Mode Control is disabled.)

For details on the Flash protect, refer to the reference manual "Flash Memory".

The target Flash memory area is specified as a contiguous area starting from block 0 in block units. A maximum of blocks 0 to 31 can be specified. The Flash write and erase commands to blocks specified as Non-releasable Flash Protect are ignored.

The following modes do not start when the Non-releasable Flash Protect is enabled:

- Single Boot Mode
- Flash Writer Mode

Also, if the Chip Protect is enabled (Both the Chip Protect bit and ***[FCCPROMR]***<CPROMSK> are "1".), the Automatic CPROTCON Releasing command is ignored.

### 3.3.2. Operation

The area setting, enable setting, and Lock Setting of the Non-releasable Flash Protect are done by the Automatic SAMNRFP Programming of the Flash command. If the Lock Setting is not set, the area setting and enable setting can be released by the Automatic SAMNRFP Releasing command. The lock Setting disables the Automatic SAMNRFP Releasing command, so that the Non-releasable Flash Protect and the Secure Access Memory cannot be released.

The status of the area setting and enable setting of the Non-releasable Flash Protect can be checked with the Non-releasable Flash Protect Status Register ***[FCNRFPSR]***.

The Lock Setting can be checked with the Lock Status Register ***[FCLOCKSR]***<LOCKSTA>.

## 3.4. TOSHIBA Test Mode Control (TCON)

### 3.4.1. Function

When the TOSHIBA Test Mode Control is enabled, our test mode and the Flash Writer Mode are prohibited.

### 3.4.2. Operation

To enable TOSHIBA Test Mode Control, execute the Automatic TCON Programming of the Flash command. To release it, execute the Automatic CPROTCON Releasing command. When executing the Automatic CPROTCON Release command, the behavior varies depending on the value of ***[FCCPROMR]***<CPROMSK>. Refer to "3.1.2.4 Operation of Chip Protect Bit".

The status of the TOSHIBA Test Mode Control can be checked with the Chip Protect /TOSHIBA Test Mode Control Status Register ***[FCCPROTCONSR]***<TCONSTA>.

## 3.5. RAM Transfer Command (Single Boot Mode)

Refer to the reference manual "Flash Memory" for details on the RAM Transfer command in the Single Boot Mode.

### 3.5.1. Function

Password authentication is performed when executing the RAM Transfer command in the Single Boot Mode.

### 3.5.2. Operation

A contiguous 255 bytes of data in the Flash memory is used as the password.

When executing a RAM Transfer command, the user is prompted to enter the start address of the data to be used as the password and 255 bytes of password data.

# 4. Example of Usage

This chapter describes a debug tool connection when using the security functions.

- Under development by user

  During the development of application software, the Chip Protection is disabled to use a debug tool.

  When using the Secure Access Memory, define the areas for each state and create a Boot state program for startup, an App state program for normal operation, and a Lib state program if necessary.

  After checking the operation of the Secure Access Memory, check its operation in conjunction with the other security functions.

  It is recommended to use the Chip Protect in conjunction with the Secure Access Memory.

  Enable the Non-releasable Flash Protect and the TOSHIBA Test Mode Control as needed. If these functions are enabled, there are restrictions on failure analysis.

  Set the lock setting when using the Secure Access Memory or the Non-releasable Flash Protect.

  Make a final operational check with all necessary security functions configured.

- Failure analysis by user

  To release the Chip Protect in order to use a debug tool in failure analysis, the following methods are available.

  – Release by CPU program execution

    A debug tool can be used by performing the following operations triggered by external communications, etc.

    - Temporary release of Chip Protect
      Chip Protect is temporarily released by setting ***[FCCPROMR]***<CPROMSK to “0”.
    - Release of Chip Protect
      The Chip Protect and TOSHIBA Test Mode Control are released by executing the Automatic CPROTCON Releasing command.

  – Forced CPROTCON release

    The Forced CPROTCON release is available when the Secure Access memory is enabled and the Non-releasable Flash Protect is disabled.
    The Forced CPROTCON release is executed by the Single Boot Mode startup operation (reset by RESET_N pin with BOOT_N input "Low") to erase the Flash memory data, release the Chip Protect, and release the TOSHIBA Test Mode Control.
    Refer to the reference manual "Secure Access Memory" for the Forced CPROTCON release.

  – Flash Memory Erasing command (Single Boot Mode)

    Executing the Flash Memory Erasing command in the Single Boot Mode erases the Flash memory data, releases the Chip Protect, releases the TOSHIBA Test Mode Control, and releases the Flash Protect.
    However, Single Boot Mode will not start if the Secure Access Memory or Non-releasable Flash Protect is enabled.

- Failure analysis by TOSHIBA
  Analysis using our test mode is not possible when the TOSHIBA Test Mode control is enabled.
  When requesting our analysis, please make sure that the TOSHIBA Test Mode Control is released.

# 5. Revision History

**Table 5.1 Revision History**

| Revision | Date | Description |
|---|---|---|
| 1.0 | 2026-01-30 | - First release |

## RESTRICTIONS ON PRODUCT USE

Toshiba Corporation and its subsidiaries and affiliates are collectively referred to as “TOSHIBA”.
Hardware, software and systems described in this document are collectively referred to as “Product”.

- TOSHIBA reserves the right to make changes to the information in this document and related Product without notice.
- This document and any information herein may not be reproduced without prior written permission from TOSHIBA. Even with TOSHIBA's written permission, reproduction is permissible only if reproduction is without alteration/omission.
- Though TOSHIBA works continually to improve Product's quality and reliability, Product can malfunction or fail. Customers are responsible for complying with safety standards and for providing adequate designs and safeguards for their hardware, software and systems which minimize risk and avoid situations in which a malfunction or failure of Product could cause loss of human life, bodily injury or damage to property, including data loss or corruption. Before customers use the Product, create designs including the Product, or incorporate the Product into their own applications, customers must also refer to and comply with (a) the latest versions of all relevant TOSHIBA information, including without limitation, this document, the specifications, the data sheets and application notes for Product and the precautions and conditions set forth in the "TOSHIBA Semiconductor Reliability Handbook" and (b) the instructions for the application with which the Product will be used with or for. Customers are solely responsible for all aspects of their own product design or applications, including but not limited to (a) determining the appropriateness of the use of this Product in such design or applications; (b) evaluating and determining the applicability of any information contained in this document, or in charts, diagrams, programs, algorithms, sample application circuits, or any other referenced documents; and (c) validating all operating parameters for such designs and applications. **TOSHIBA ASSUMES NO LIABILITY FOR CUSTOMERS' PRODUCT DESIGN OR APPLICATIONS.**
- **PRODUCT IS NEITHER INTENDED NOR WARRANTED FOR USE IN EQUIPMENTS OR SYSTEMS THAT REQUIRE EXTRAORDINARILY HIGH LEVELS OF QUALITY AND/OR RELIABILITY, AND/OR A MALFUNCTION OR FAILURE OF WHICH MAY CAUSE LOSS OF HUMAN LIFE, BODILY INJURY, SERIOUS PROPERTY DAMAGE AND/OR SERIOUS PUBLIC IMPACT ("UNINTENDED USE").** Except for specific applications as expressly stated in this document, Unintended Use includes, without limitation, equipment used in nuclear facilities, equipment used in the aerospace industry, lifesaving and/or life supporting medical equipment, equipment used for automobiles, trains, ships and other transportation, traffic signaling equipment, equipment used to control combustions or explosions, safety devices, elevators and escalators, and devices related to power plant. **IF YOU USE PRODUCT FOR UNINTENDED USE, TOSHIBA ASSUMES NO LIABILITY FOR PRODUCT.** For details, please contact your TOSHIBA sales representative or contact us via our website.
- Do not disassemble, analyze, reverse-engineer, alter, modify, translate or copy Product, whether in whole or in part.
- Product shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable laws or regulations.
- The information contained herein is presented only as guidance for Product use. No responsibility is assumed by TOSHIBA for any infringement of patents or any other intellectual property rights of third parties that may result from the use of Product. No license to any intellectual property right is granted by this document, whether express or implied, by estoppel or otherwise.
- **ABSENT A WRITTEN SIGNED AGREEMENT, EXCEPT AS PROVIDED IN THE RELEVANT TERMS AND CONDITIONS OF SALE FOR PRODUCT, AND TO THE MAXIMUM EXTENT ALLOWABLE BY LAW, TOSHIBA (1) ASSUMES NO LIABILITY WHATSOEVER, INCLUDING WITHOUT LIMITATION, INDIRECT, CONSEQUENTIAL, SPECIAL, OR INCIDENTAL DAMAGES OR LOSS, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, LOSS OF OPPORTUNITIES, BUSINESS INTERRUPTION AND LOSS OF DATA, AND (2) DISCLAIMS ANY AND ALL EXPRESS OR IMPLIED WARRANTIES AND CONDITIONS RELATED TO SALE, USE OF PRODUCT, OR INFORMATION, INCLUDING WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OF INFORMATION, OR NONINFRINGEMENT.**
- Do not use or otherwise make available Product or related software or technology for any military purposes, including without limitation, for the design, development, use, stockpiling or manufacturing of nuclear, chemical, or biological weapons or missile technology products (mass destruction weapons). Product and related software and technology may be controlled under the applicable export laws and regulations including, without limitation, the Japanese Foreign Exchange and Foreign Trade Law and the U.S. Export Administration Regulations. Export and re-export of Product or related software or technology are strictly prohibited except in compliance with all applicable export laws and regulations.
- Please contact your TOSHIBA sales representative for details as to environmental matters such as the RoHS compatibility of Product. Please use Product in compliance with all applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive. **TOSHIBA ASSUMES NO LIABILITY FOR DAMAGES OR LOSSES OCCURRING AS A RESULT OF NONCOMPLIANCE WITH APPLICABLE LAWS AND REGULATIONS.**