

Xilinx Standalone Library Documentation

XilSKey Library v6.6

UG1191 (2018.3) November 14, 2018

Table of Contents

Chapter 1: Overview

Hardware Setup	6
Hardware setup for Zynq PL	6
Hardware setup for UltraScale or UltraScale+	8
Source Files	8

Chapter 2: BBRAM PL API

Overview	10
Example Usage	10
Function Documentation	11
XiISKey_Bbram_Program	11

Chapter 3: Zynq UltraScale+ MPSoC BBRAM PS API

Overview	12
Example Usage	12
Function Documentation	12
XiISKey_ZynqMp_Bbram_Program	12
XiISKey_ZynqMp_Bbram_Zeroise	13

Chapter 4: Zynq eFUSE PS API

Overview	14
Example Usage	14
Function Documentation	14
XiISKey_EfusePs_Write	14
XiISKey_EfusePs_Read	15
XiISKey_EfusePs_ReadStatus	15

Chapter 5: Zynq UltraScale+ MPSoC eFUSE PS API

Overview	17
Example Usage	17
Data Structure Documentation	18
struct XiISKey_Efuse	18

Function Documentation	18
XiISKey_ZynqMp_EfusePs_CheckAesKeyCrc	18
XiISKey_ZynqMp_EfusePs_ReadUserFuse	19
XiISKey_ZynqMp_EfusePs_ReadPpk0Hash	19
XiISKey_ZynqMp_EfusePs_ReadPpk1Hash	19
XiISKey_ZynqMp_EfusePs_ReadSpkId	20
XiISKey_ZynqMp_EfusePs_ReadDna	20
XiISKey_ZynqMp_EfusePs_ReadSecCtrlBits	21
XiISKey_ZynqMp_EfusePs_Write	21
XiISKey_ZynqMpEfuseAccess	22
XiISKey_ZynqMp_EfusePs_WritePufHelpData	22
XiISKey_ZynqMp_EfusePs_ReadPufHelpData	22
XiISKey_ZynqMp_EfusePs_WritePufChash	23
XiISKey_ZynqMp_EfusePs_ReadPufChash	23
XiISKey_ZynqMp_EfusePs_WritePufAux	24
XiISKey_ZynqMp_EfusePs_ReadPufAux	24
XiISKey_Write_Puf_EfusePs_SecureBits	25
XiISKey_Read_Puf_EfusePs_SecureBits	25
XiISKey_Puf_Debug2	25
XiISKey_Puf_Registration	26
XiISKey_Puf_Regeneration	26
 Chapter 6: eFUSE PL API	
Overview	27
Example Usage	27
Function Documentation	27
XiISKey_EfusePI_Program	27
XiISKey_EfusePI_ReadStatus	28
XiISKey_EfusePI_ReadKey	28
 Chapter 7: CRC Calculation API	
Overview	30
Function Documentation	30
XiISKey_CrcCalculation	30
XiISKey_CrcCalculation_AesKey	31
 Chapter 8: User-Configurable Parameters	
Overview	32
Zynq User-Configurable PS eFUSE Parameters	32
Zynq User-Configurable PL eFUSE Parameters	34

Overview	34
MIO Pins for Zynq PL eFUSE JTAG Operations	35
MUX Selection Pin for Zynq PL eFUSE JTAG Operations	37
MUX Parameter for Zynq PL eFUSE JTAG Operations	37
AES and User Key Parameters	38
Zynq User-Configurable PL BBRAM Parameters	39
Overview	39
MUX Parameter for Zynq BBRAM PL JTAG Operations	40
AES and User Key Parameters	40
UltraScale or UltraScale+ User-Configurable BBRAM PL Parameters	40
Overview	40
AES Keys and Related Parameters	40
DPA Protection for BBRAM key	42
GPIO Pins Used for PL Master JTAG and HWM Signals	42
GPIO Channels	42
UltraScale or UltraScale+ User-Configurable PL eFUSE Parameters	43
Overview	43
GPIO Pins Used for PL Master JTAG Signal	45
GPIO Channels	46
AES Keys and Related Parameters	46
Zynq UltraScale+ MPSoC User-Configurable PS eFUSE Parameters	49
Overview	49
AES Keys and Related Parameters	51
User Keys and Related Parameters	52
PPK0 Keys and Related Parameters	56
PPK1 Keys and Related Parameters	57
SPK ID and Related Parameters	58
Zynq UltraScale+ MPSoC User-Configurable PS BBRAM Parameters	60
Zynq UltraScale+ MPSoC User-Configurable PS PUF Parameters	60
 Chapter 9: Error Codes	
Overview	63
PL eFUSE Error Codes	63
PS eFUSE Error Codes	66
Zynq UltraScale+ MPSoC BBRAM PS Error Codes	71
 Chapter 10: Status Codes	
 Chapter 11: Procedures	

Zynq eFUSE Writing Procedure Running from DDR as an Application	73
Zynq eFUSE Driver Compilation Procedure for OCM	73
UltraScale eFUSE Access Procedure	74
UltraScale BBRAM Access Procedure	74

Appendix A: Additional Resources and Legal Notices

Overview

The XilSKey library provides APIs for programming and reading eFUSE bits and for programming the battery-backed RAM (BBRAM) of Zynq®-7000 SoC, UltraScale™, UltraScale+™ and the Zynq UltraScale+ MPSoC devices.

- In Zynq-7000 devices:
 - PS eFUSE holds the RSA primary key hash bits and user feature bits, which can enable or disable some Zynq-7000 processor features.
 - PL eFUSE holds the AES key, the user key and some of the feature bits.
 - PL BBRAM holds the AES key.
- In UltraScale or UltraScale+:
 - PL eFuse holds the AES key, 32 bit and 128 bit user key, RSA hash and some of the feature bits.
 - PL BBRAM holds AES key with or without DPA protection enable or obfuscated key programming.
- In Zynq UltraScale+ MPSoC:
 - PS eFUSE holds the AES key, the user fuses, PPK0 and PPK1 hash, SPK ID and some user feature bits which can be used to enable or disable some Zynq UltraScale+ MPSoC features.
 - BBRAM holds the AES key.

Hardware Setup

This section describes the hardware setup required for programming PL BBRAM or PL eFUSE.

Hardware setup for Zynq PL

This chapter describes the hardware setup required for programming BBRAM or eFUSE of Zynq PL devices. PL eFUSE or PL BBRAM is accessed through PS via MIO pins which are used for communication PL eFUSE or PL BBRAM through JTAG signals, these can be changed depending on the hardware setup.

A hardware setup which dedicates four MIO pins for JTAG signals should be used and the MIO pins should be mentioned in application header file (xilskey_input.h). There should be a method to download this example and have the MIO pins connected to JTAG before running this application. You can change the listed pins at your discretion.

Hardware setup for UltraScale or UltraScale+

This chapter describes the hardware setup required for programming BBRAM or eFUSE of UltraScale devices. Accessing UltraScale MicroBlaze eFuse is done by using block RAM initialization. UltraScale eFUSE programming is done through MASTER JTAG. Crucial Programming sequence will be taken care by Hardware module. It is mandatory to add Hardware module in the design. Use hardware module's vhd code and instructions provided to add Hardware module in the design.

- You need to add the Master JTAG primitive to design, that is, the MASTER_JTAG_inst instantiation has to be performed and AXI GPIO pins have to be connected to TDO, TDI, TMS and TCK signals of the MASTER_JTAG primitive.
- For programming eFUSE, along with master JTAG, hardware module(HWM) has to be added in design and it's signals XSK_EFUSEPL_AXI_GPIO_HWM_READY , XSK_EFUSEPL_AXI_GPIO_HWM_END and XSK_EFUSEPL_AXI_GPIO_HWM_START, needs to be connected to AXI GPIO pins to communicate with HWM. Hardware module is not mandatory for programming BBRAM. If your design has a HWM, it is not harmful for accessing BBRAM.
- All inputs (Master JTAG's TDO and HWM's HWM_READY, HWM_END) and all outputs (Master JTAG TDI, TMS, TCK and HWM's HWM_START) can be connected in one channel (or) inputs in one channel and outputs in other channel.
- Some of the outputs of GPIO in one channel and some others in different channels are not supported.
- The design should contain AXI BRAM control memory mapped (1MB).

Note

MASTER_JTAG will disable all other JTAGs.

For providing inputs of MASTER JTAG signals and HWM signals connected to the GPIO pins and GPIO channels, refer GPIO Pins Used for PL Master JTAG Signal and GPIO Channels sections of the UltraScale User-Configurable PL eFUSE Parameters and UltraScale User-Configurable PL BBRAM Parameters.

The procedure for programming BBRAM of eFUSE of UltraScale or UltraScale+ can be referred at UltraScale BBRAM Access Procedure and UltraScale eFUSE Access Procedure.

Source Files

The following is a list of eFUSE and BBRAM application project files, folders and macros.

- `xilskey_efuse_example.c`: This file contains the main application code. The file helps in the PS/PL structure initialization and writes/reads the PS/PL eFUSE based on the user settings provided in the `xilskey_input.h` file.
- `xilskey_input.h`: This file contains all the actions that are supported by the eFUSE library. Using the preprocessor directives given in the file, you can read/write the bits in the PS/PL eFUSE. More explanation of each directive is provided in the following sections. Burning or reading the PS/PL eFUSE bits is based on the values set in the `xilskey_input.h` file. Also contains GPIO pins and channels connected to MASTER JTAG primitive and hardware module to access Ultrascale eFUSE.

In this file:

- specify the 256 bit key to be programmed into BBRAM.
- specify the AES(256 bit) key, User (32 bit and 128 bit) keys and RSA key hash(384 bit) key to be programmed into UltraScale eFUSE.
- XSK_EFUSEPS_DRIVER: Define to enable the writing and reading of PS eFUSE.
- XSK_EFUSEPL_DRIVER: Define to enable the writing of PL eFUSE.
- `xilskey_bbram_example.c`: This file contains the example to program a key into BBRAM and verify the key.

Note

This algorithm only works when programming and verifying key are both executed in the recommended order.

- `xilskey_efuseps_zynqmp_example.c`: This file contains the example code to program the PS eFUSE and read back of eFUSE bits from the cache.
- `xilskey_efuseps_zynqmp_input.h`: This file contains all the inputs supported for eFUSE PS of Zynq UltraScale+ MPSoC. eFUSE bits are programmed based on the inputs from the `xilskey_efuseps_zynqmp_input.h` file.
- `xilskey_bbramps_zynqmp_example.c`: This file contains the example code to program and verify BBRAM key. Default is zero. You can modify this key on top of the file.
- `xilskey_bbram_ultrascale_example.c`: This file contains example code to program and verify BBRAM key of UltraScale.

Note

Programming and verification of BBRAM key cannot be done separately.

- `xilskey_bbram_ultrascale_input.h`: This file contains all the preprocessor directives you need to provide. In this file, specify BBRAM AES key or Obfuscated AES key to be programmed, DPA protection enable and, GPIO pins and channels connected to MASTER JTAG primitive.
- `xilskey_puf_registration.c`: This file contains all the PUF related code. This example illustrates PUF registration and generating black key and programming eFUSE with PUF helper data, CHash and Auxiliary data along with the Black key.
- `xilskey_puf_registration.h`: This file contains all the preprocessor directives based on which read/write the eFUSE bits and Syndrome data generation. More explanation of each directive is provided in the following sections.



WARNING: *Ensure that you enter the correct information before writing or 'burning' eFUSE bits. Once burned, they cannot be changed. The BBRAM key can be programmed any number of times.*

Note

POR reset is required for the eFUSE values to be recognized.

BBRAM PL API

Overview

This chapter provides a linked summary and detailed descriptions of the battery-backed RAM (BBRAM) APIs of Zynq® PL and UltraScale™ devices.

Example Usage

- Zynq BBRAM PL example usage:
 - The Zynq BBRAM PL example application should contain the `xilskey_bbram_example.c` and `xilskey_input.h` files.
 - You should provide user configurable parameters in the `xilskey_input.h` file. For more information, refer [Zynq User-Configurable PL BBRAM Parameters](#).
- UltraScale BBRAM example usage:
 - The UltraScale BBRAM example application should contain the `xilskey_bbram_ultrascale_input.h` and `xilskey_bbram_ultrascale_example.c` files.
 - You should provide user configurable parameters in the `xilskey_bbram_ultrascale_input.h` file. For more information, refer [UltraScale or UltraScale+ User-Configurable BBRAM PL Parameters](#).

Note

It is assumed that you have set up your hardware prior to working on the example application. For more information, refer [Hardware Setup](#).

Functions

- int [XilSKey_Bbram_Program](#) (XilSKey_Bbram *InstancePtr)

Function Documentation

int XilSKey_Bbram_Program (XilSKey_Bbram * *InstancePtr*)

This function implements the BBRAM algorithm for programming and verifying key.
The program and verify will only work together in and in that order.

Parameters

<i>InstancePtr</i>	Pointer to XilSKey_Bbram
--------------------	--------------------------

Returns

- XST_FAILURE - In case of failure
- XST_SUCCESS - In case of Success

Note

This function will program BBRAM of Ultrascale and Zynq as well.

Zynq UltraScale+ MPSoC BBRAM PS API

Overview

This chapter provides a linked summary and detailed descriptions of the battery-backed RAM (BBRAM) APIs for Zynq® UltraScale+™ MPSoC devices.

Example Usage

- The Zynq UltraScale+ MPSoC example application should contain the `xilsky_bbramps_zynqmp_example.c` file.
- User configurable key can be modified in the same file (`xilsky_bbramps_zynqmp_example.c`), at the `XSK_ZYNQMP_BBRAMPS_AES_KEY` macro.

Functions

- `u32 XilSKey_ZynqMp_Bbram_Program (u32 *AesKey)`
- `void XilSKey_ZynqMp_Bbram_Zeroise ()`

Function Documentation

u32 XilSKey_ZynqMp_Bbram_Program (u32 * AesKey)

This function implements the BBRAM programming and verifying the key written. Program and verification of AES will work only together. CRC of the provided key will be calculated internally and verified after programming.

Parameters

<i>AesKey</i>	Pointer to the key which has to be programmed.
---------------	--

Returns

- Error code from `XskZynqMp_Ps_Bbram_ErrorCodes` enum if it fails
- `XST_SUCCESS` if programming is done.



void XilSKey_ZynqMp_Bbram_Zeroise ()

This function zeroize's Bbram Key.

Parameters

None.	
-------	--

Returns

None.

Note

BBRAM key will be zeroized.

Zynq eFUSE PS API

Overview

This chapter provides a linked summary and detailed descriptions of the Zynq eFUSE PS APIs.

Example Usage

- The Zynq eFUSE PS example application should contain the `xilsky_efuse_example.c` and the `xilsky_input.h` files.
- There is no need of any hardware setup. By default, both the eFUSE PS and PL are enabled in the application. You can comment 'XSK_EFUSEPL_DRIVER' to execute only the PS. For more details, refer [Zynq User-Configurable PS eFUSE Parameters](#).

Functions

- u32 [XilSKey_EfusePs_Write](#) (XilSKey_EPs *PsInstancePtr)
- u32 [XilSKey_EfusePs_Read](#) (XilSKey_EPs *PsInstancePtr)
- u32 [XilSKey_EfusePs_ReadStatus](#) (XilSKey_EPs *InstancePtr, u32 *StatusBits)

Function Documentation

u32 XilSKey_EfusePs_Write (XilSKey_EPs * *InstancePtr*)

PS eFUSE interface functions.

PS eFUSE interface functions.

Parameters

<i>InstancePtr</i>	Pointer to the PsEfuseHandle which describes which PS eFUSE bit should be burned.
--------------------	---

Returns

- XST_SUCCESS.
- In case of error, value is as defined in xilskey_utils.h. Error value is a combination of Upper 8 bit value and Lower 8 bit value. For example, 0x8A03 should be checked in error.h as 0x8A00 and 0x03. Upper 8 bit value signifies the major error and lower 8 bit values tell more precisely.

Note

When called, this initializes the timer, XADC subsystems. Unlocks the PS eFUSE controller. Configures the PS eFUSE controller. Writes the hash and control bits if requested. Programs the PS eFUSE to enable the RSA authentication if requested. Locks the PS eFUSE controller. Returns an error, if the reference clock frequency is not in between 20 and 60 MHz or if the system is not in a position to write the requested PS eFUSE bits (because the bits are already written or not allowed to write) or if the temperature and voltage are not within range.

u32 XilSKey_EfusePs_Read (XilSKey_EPs * InstancePtr)

This function is used to read the PS eFUSE.

Parameters

<i>InstancePtr</i>	Pointer to the PsEfuseHandle which describes which PS eFUSE should be burned.
--------------------	---

Returns

- XST_SUCCESS no errors occurred.
- In case of error, value is as defined in xilskey_utils.h. Error value is a combination of Upper 8 bit value and Lower 8 bit value. For example, 0x8A03 should be checked in error.h as 0x8A00 and 0x03. Upper 8 bit value signifies the major error and lower 8 bit values tell more precisely.

Note

When called: This API initializes the timer, XADC subsystems. Unlocks the PS eFUSE Controller. Configures the PS eFUSE Controller and enables read-only mode. Reads the PS eFUSE (Hash Value), and enables read-only mode. Locks the PS eFUSE Controller. Returns an error, if the reference clock frequency is not in between 20 and 60MHz. or if unable to unlock PS eFUSE controller or requested address corresponds to restricted bits. or if the temperature and voltage are not within range.

u32 XilSKey_EfusePs_ReadStatus (XilSKey_EPs * InstancePtr, u32 * StatusBits)

This function is used to read the PS efuse status register.

Parameters

<i>InstancePtr</i>	Pointer to the PS eFUSE instance.
<i>StatusBits</i>	Buffer to store the status register read.

Returns

- XST_SUCCESS.
- XST_FAILURE

Note

This API unlocks the controller and reads the Zynq PS eFUSE status register.

Zynq UltraScale+ MPSoC eFUSE PS API

Overview

This chapter provides a linked summary and detailed descriptions of the Zynq MPSoC UltraScale+ eFUSE PS APIs.

Example Usage

- For programming eFUSE other than PUF, the Zynq UltraScale+ MPSoC example application should contain the `xilsky_efuseps_zynqmp_example.c` and the `xilsky_efuseps_zynqmp_input.h` files.
 - For PUF registration and programming PUF, the the Zynq UltraScale+ MPSoC example application should contain the `xilsky_puf_registration.c` and the `xilsky_puf_registration.h` files.
 - For more details on the user configurable parameters, refer [Zynq UltraScale+ MPSoC User-Configurable PS eFUSE Parameters](#) and [Zynq UltraScale+ MPSoC User-Configurable PS PUF Parameters](#).
-

Data Structures

- struct [XilSKey_Efuse](#)
-

Functions

- u32 [XilSKey_ZynqMp_EfusePs_CheckAesKeyCrc](#) (u32 CrcValue)
- u32 [XilSKey_ZynqMp_EfusePs_ReadUserFuse](#) (u32 *UseFusePtr, u8 UserFuse_Num, u8 ReadOption)
- u32 [XilSKey_ZynqMp_EfusePs_ReadPpk0Hash](#) (u32 *Ppk0Hash, u8 ReadOption)
- u32 [XilSKey_ZynqMp_EfusePs_ReadPpk1Hash](#) (u32 *Ppk1Hash, u8 ReadOption)
- u32 [XilSKey_ZynqMp_EfusePs_ReadSpkId](#) (u32 *SpkId, u8 ReadOption)
- void [XilSKey_ZynqMp_EfusePs_ReadDna](#) (u32 *DnaRead)
- u32 [XilSKey_ZynqMp_EfusePs_ReadSecCtrlBits](#) (XilSKey_SecCtrlBits *ReadBackSecCtrlBits, u8 ReadOption)
- u32 [XilSKey_ZynqMp_EfusePs_Write](#) (XilSKey_ZynqMpEPs *InstancePtr)
- u32 [XilSKey_ZynqMpEfuseAccess](#) (const u32 AddrHigh, const u32 AddrLow)
- u32 [XilSKey_ZynqMp_EfusePs_WritePufHelpData](#) (XilSKey_Puf *InstancePtr)

- u32 [XilSKey_ZynqMp_EfusePs_ReadPufHelperData](#) (u32 *Address)
- u32 [XilSKey_ZynqMp_EfusePs_WritePufChash](#) (XilSKey_Puf *InstancePtr)
- u32 [XilSKey_ZynqMp_EfusePs_ReadPufChash](#) (u32 *Address, u8 ReadOption)
- u32 [XilSKey_ZynqMp_EfusePs_WritePufAux](#) (XilSKey_Puf *InstancePtr)
- u32 [XilSKey_ZynqMp_EfusePs_ReadPufAux](#) (u32 *Address, u8 ReadOption)
- u32 [XilSKey_Write_Puf_EfusePs_SecureBits](#) (XilSKey_Puf_Secure *WriteSecureBits)
- u32 [XilSKey_Read_Puf_EfusePs_SecureBits](#) (XilSKey_Puf_Secure *SecureBitsRead, u8 ReadOption)
- u32 [XilSKey_Puf_Debug2](#) (XilSKey_Puf *InstancePtr)
- u32 [XilSKey_Puf_Registration](#) (XilSKey_Puf *InstancePtr)
- u32 [XilSKey_Puf_Regeneration](#) (XilSKey_Puf *InstancePtr)

Data Structure Documentation

struct XilSKey_Efuse

[XilSKey_Efuse](#) is the eFUSE access structure.

Using this structure, user can request the eFUSE access via IPI response.

Data Fields

u64	Src	Address of Data buffer.
u32	Size	Size in words.
u32	Offset	offset
u32	Flag	Flag - 0 : to read efuse and Flag - 1 : to write efuse.

Function Documentation

u32 XilSKey_ZynqMp_EfusePs_CheckAesKeyCrc (u32 CrcValue)

This function performs CRC check of AES key.

Parameters

<i>CrcValue</i>	A 32 bit CRC value of an expected AES key.
-----------------	--

Returns

- XST_SUCCESS on successful CRC check.
- ErrorCode on failure

Note

For Calculating CRC of AES key use [XilSKey_CrcCalculation\(\)](#) API or [XilSKey_CrcCalculation_AesKey\(\)](#) API.

u32 XilSKey_ZynqMp_EfusePs_ReadUserFuse (u32 * UseFusePtr, u8 UserFuse_Num, u8 ReadOption)

This function is used to read user fuse from efuse or cache based on user's read option.

Parameters

<i>UseFusePtr</i>	Pointer to an array which holds the readback user fuse in.
<i>UserFuse_Num</i>	A variable which holds the user fuse number. Range is (User fuses: 0 to 7)
<i>ReadOption</i>	A variable which has to be provided by user based on this input reading is happend from cache or from efuse array. <ul style="list-style-type: none"> • 0 Reads from cache • 1 Reads from efuse array

Returns

- XST_SUCCESS on successful read
- ErrorCode on failure

u32 XilSKey_ZynqMp_EfusePs_ReadPpk0Hash (u32 * Ppk0Hash, u8 ReadOption)

This function is used to read PPK0 hash from efuse or cache based on user's read option.

Parameters

<i>Ppk0Hash</i>	A pointer to an array which holds the readback PPK0 hash in.
<i>ReadOption</i>	A variable which has to be provided by user based on this input reading is happend from cache or from efuse array. <ul style="list-style-type: none"> • 0 Reads from cache • 1 Reads from efuse array

Returns

- XST_SUCCESS on successful read
- ErrorCode on failure

u32 XilSKey_ZynqMp_EfusePs_ReadPpk1Hash (u32 * Ppk1Hash, u8 ReadOption)

This function is used to read PPK1 hash from efuse or cache based on user's read option.

Parameters

<i>Ppk1Hash</i>	Pointer to an array which holds the readback PPK1 hash in.
<i>ReadOption</i>	<p>A variable which has to be provided by user based on this input reading is happend from cache or from efuse array.</p> <ul style="list-style-type: none"> • 0 Reads from cache • 1 Reads from efuse array

Returns

- XST_SUCCESS on successful read
- ErrorCode on failure

u32 XilSKey_ZynqMp_EfusePs_ReadSpkId (u32 * *SpkId*, u8 *ReadOption*)

This function is used to read SPKID from efuse or cache based on user's read option.

Parameters

<i>SpkId</i>	Pointer to a 32 bit variable which holds SPK ID.
<i>ReadOption</i>	<p>A variable which has to be provided by user based on this input reading is happend from cache or from efuse array.</p> <ul style="list-style-type: none"> • 0 Reads from cache • 1 Reads from efuse array

Returns

- XST_SUCCESS on successful read
- ErrorCode on failure

void XilSKey_ZynqMp_EfusePs_ReadDna (u32 * *DnaRead*)

This function is used to read DNA from efuse.

Parameters

<i>DnaRead</i>	Pointer to 32 bit variable which holds the readback DNA in.
----------------	---

Returns

None.

u32 XilSKey_ZynqMp_EfusePs_ReadSecCtrlBits (XilSKey_SecCtrlBits * *ReadBackSecCtrlBits*, u8 *ReadOption*)

This function is used to read the PS efuse secure control bits from cache or eFUSE based on user input provided.

Parameters

<i>ReadBackSecCtrlBits</i>	Pointer to the XilSKey_SecCtrlBits which holds the read secure control bits.
<i>ReadOption</i>	Variable which has to be provided by user based on this input reading is happend from cache or from efuse array. <ul style="list-style-type: none"> • 0 Reads from cache • 1 Reads from efuse array

Returns

- XST_SUCCESS if reads successfully
- XST_FAILURE if reading is failed

Note

Cache reload is required for obtaining updated values for ReadOption 0.

u32 XilSKey_ZynqMp_EfusePs_Write (XilSKey_ZynqMpEPs * *InstancePtr*)

This function is used to program the PS efuse of ZynqMP, based on user inputs.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_ZynqMpEPs.
--------------------	-----------------------------------

Returns

- XST_SUCCESS if programs successfully.
- Errorcode on failure

Note

On successful efuse programming cache is been reloaded, so programmed efuse bits can directly read from efuse cache.

u32 XilSKey_ZynqMpEfuseAccess (const u32 AddrHigh, const u32 AddrLow)

This function provides access to efuse memory.

Parameters

<i>AddrHigh</i>	Higher 32-bit address of the XilSKey_Efuse structure.
<i>AddrLow</i>	Lower 32-bit address of the XilSKey_Efuse structure.

Returns

- XST_SUCCESS - On success
- ErrorCode - on Failure

Note

This function is for programming efuse through IPI response it has corresponding IPI response call in PMUFW.

u32 XilSKey_ZynqMp_EfusePs_WritePufHelprData (XilSKey_Puf * InstancePtr)

This function programs the PS efuse's with puf helper data of ZynqMp.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if programs successfully.
- Errorcode on failure

Note

To generate PufSyndromeData please use XilSKey_Puf_Registration API

u32 XilSKey_ZynqMp_EfusePs_ReadPufHelprData (u32 * Address)

This function reads the puf helper data from eFUSE.

Parameters

<i>Address</i>	Pointer to data array which holds the Puf helper data read from ZynqMp efuse.
----------------	---

Returns

- XST_SUCCESS if reads successfully.
- Errorcode on failure.

Note

This function only reads from eFUSE non-volatile memory. There is no option to read from Cache.

u32 XilSKey_ZynqMp_EfusePs_WritePufChash (XilSKey_Puf * *InstancePtr*)

This API programs eFUSE with CHash value.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if chash is programmed successfully.
- Errorcode on failure

Note

To generate CHash value please use XilSKey_Puf_Registration API

u32 XilSKey_ZynqMp_EfusePs_ReadPufChash (u32 * *Address*, u8 *ReadOption*)

This API reads efuse puf CHash Data from efuse array or cache based on the user read option.

Parameters

<i>Address</i>	Pointer which holds the read back value of chash
<i>ReadOption</i>	<p>A u8 variable which has to be provided by user based on this input reading is happend from cache or from efuse array.</p> <ul style="list-style-type: none"> • 0(XSK_EFUSEPS_READ_FROM_CACHE)Reads from cache • 1(XSK_EFUSEPS_READ_FROM_EFUSE)Reads from efuse array

Returns

- XST_SUCCESS if programs successfully.
- Errorcode on failure

Note

Cache reload is required for obtaining updated values for ReadOption 0.

u32 XilSKey_ZynqMp_EfusePs_WritePufAux (XilSKey_Puf * InstancePtr)

This API programs efuse puf Auxiliary Data.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if programs successfully.
- Errorcode on failure

Note

To generate Auxiliary data please use the below API u32 [XilSKey_Puf_Registration\(XilSKey_Puf *InstancePtr\)](#)

u32 XilSKey_ZynqMp_EfusePs_ReadPufAux (u32 * Address, u8 ReadOption)

This API reads efuse puf Auxiliary Data from efuse array or cache based on user read option.

Parameters

<i>Address</i>	Pointer which holds the read back value of Auxiliary
<i>ReadOption</i>	<p>A u8 variable which has to be provided by user based on this input reading is happend from cache or from efuse array.</p> <ul style="list-style-type: none"> • 0(XSK_EFUSEPS_READ_FROM_CACHE)Reads from cache • 1(XSK_EFUSEPS_READ_FROM_EFUSE)Reads from efuse array

Returns

- XST_SUCCESS if programs successfully.
- Errorcode on failure

Note

Cache reload is required for obtaining updated values for ReadOption 0.

u32 XilSKey_Write_Puf_EfusePs_SecureBits (XilSKey_Puf_Secure * WriteSecureBits)

This function programs the eFUSE PUF secure bits.

Parameters

<i>WriteSecureBits</i>	Pointer to the XilSKey_Puf_Secure structure
------------------------	---

Returns

XST_SUCCESS - On success ErrorCode - on Failure

u32 XilSKey_Read_Puf_EfusePs_SecureBits (XilSKey_Puf_Secure * SecureBitsRead, u8 ReadOption)

This function is used to read the PS efuse PUF secure bits from cache or from eFUSE array based on user selection.

Parameters

<i>SecureBits</i>	Pointer to the XilSKey_Puf_Secure which holds the read eFUSE secure bits of PUF.
<i>ReadOption</i>	A u8 variable which has to be provided by user based on this input reading is happened from cache or from efuse array. <ul style="list-style-type: none"> 0(XSK_EFUSEPS_READ_FROM_CACHE) Reads from cache 1(XSK_EFUSEPS_READ_FROM_EFUSE) Reads from efuse array

Returns

XST_SUCCESS - On success ErrorCode - on Failure

u32 XilSKey_Puf_Debug2 (XilSKey_Puf * InstancePtr)

PUF Debug 2 operation.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if debug 2 mode was successful.
- ERROR if registration was unsuccessful.

Note

Updates the Debug 2 mode result @ InstancePtr->Debug2Data

u32 XilSKey_Puf_Registration (XilSKey_Puf * *InstancePtr*)

PUF Registration/Re-registration.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if registration/re-registration was successful.
- ERROR if registration was unsuccessful

Note

Updates the syndrome data @ InstancePtr->SyndromeData

u32 XilSKey_Puf_Regeneration (XilSKey_Puf * *InstancePtr*)

PUF Re-generation.

Parameters

<i>InstancePtr</i>	Pointer to the XilSKey_Puf instance.
--------------------	--------------------------------------

Returns

- XST_SUCCESS if regeneration was successful.
- ERROR if regeneration was unsuccessful

eFUSE PL API

Overview

This chapter provides a linked summary and detailed descriptions of the eFUSE APIs of Zynq eFUSE PL and UltraScale eFUSE.

Example Usage

- The Zynq eFUSE PL and UltraScale example application should contain the `xilsky_efuse_example.c` and the `xilsky_input.h` files.
- By default, both the eFUSE PS and PL are enabled in the application. You can comment 'XSK_EFUSEPL_DRIVER' to execute only the PS.
- For UltraScale, it is mandatory to comment 'XSK_EFUSEPS_DRIVER' else the example will generate an error.
- For more details on the user configurable parameters, refer [Zynq User-Configurable PL eFUSE Parameters](#) and [UltraScale or UltraScale+ User-Configurable PL eFUSE Parameters](#).
- Requires hardware setup to program PL eFUSE of Zynq or UltraScale.

Functions

- u32 [XilSKey_EfusePI_Program](#) (XilSKey_EPI *PIInstancePtr)
- u32 [XilSKey_EfusePI_ReadStatus](#) (XilSKey_EPI *InstancePtr, u32 *StatusBits)
- u32 [XilSKey_EfusePI_ReadKey](#) (XilSKey_EPI *InstancePtr)

Function Documentation

u32 XilSKey_EfusePI_Program (XilSKey_EPI * *InstancePtr*)

Programs PL eFUSE with input data given through InstancePtr.

Parameters

<i>InstancePtr</i>	Pointer to PL eFUSE instance which holds the input data to be written to PL eFUSE.
--------------------	--

Returns

- XST_FAILURE - In case of failure
- XST_SUCCESS - In case of Success

Note

When this API is called: Initializes the timer, XADC/xsysmon and JTAG server subsystems. Returns an error in the following cases, if the reference clock frequency is not in the range or if the PL DAP ID is not identified, if the system is not in a position to write the requested PL eFUSE bits (because the bits are already written or not allowed to write) if the temperature and voltage are not within range.

u32 XilSKey_EfusePI_ReadStatus (XilSKey_EPI * *InstancePtr*, u32 * *StatusBits*)

Reads the PL efuse status bits and gets all secure and control bits.

Parameters

<i>InstancePtr</i>	Pointer to PL eFUSE instance.
<i>StatusBits</i>	Buffer to store the status bits read.

Returns

- XST_FAILURE - In case of failure
- XST_SUCCESS - In case of Success

u32 XilSKey_EfusePI_ReadKey (XilSKey_EPI * *InstancePtr*)

Reads the PL efuse keys and stores them in the corresponding arrays in instance structure.

Parameters

<i>InstancePtr</i>	Pointer to PL eFUSE instance.
--------------------	-------------------------------

Returns

- XST_FAILURE - In case of failure
- XST_SUCCESS - In case of Success

Note

This function initializes the timer, XADC and JTAG server subsystems, if not already done so. In Zynq - Reads AES key and User keys. In Ultrascale - Reads 32 bit and 128 bit User keys and RSA hash But AES key cannot be read directly it can be verified with CRC check (for that we need to update the instance with 32 bit CRC value, API updates whether provided CRC value is matched with actuals or not). To calculate the CRC of expected AES key one can use any of the following APIs [XilSKey_CrcCalculation\(\)](#) or [XilSKey_CrcCalculation_AesKey\(\)](#)

CRC Calculation API

Overview

This chapter provides a linked summary and detailed descriptions of the CRC calculation APIs. For UltraScale and Zynq UltraScale+ MPSoC devices, programmed AES cannot be read back. The programmed AES key can only be confirmed by doing CRC check of AES key.

Functions

- u32 [XilSKey_CrcCalculation](#) (u8 *Key)
- u32 [XilSKey_CrcCalculation_AesKey](#) (u8 *Key)

Function Documentation

u32 XilSKey_CrcCalculation (u8 * Key)

Calculates CRC value of provided key, this API expects key in string format.

Parameters

<i>Key</i>	Pointer to the string contains AES key in hexa decimal of length less than or equal to 64.
------------	--

Returns

- On Success returns the Crc of AES key value.
- On failure returns the error code when string length is greater than 64

Note

This API calculates CRC of AES key for Ultrascale Microblaze's PL eFuse and ZynqMp UltraScale PS eFuse. If length of the string provided is lesser than 64, API appends the string with zeros.

u32 XilSkey_CrcCalculation_AesKey (u8 * Key)

Calculates CRC value of the provided key.
Key should be provided in hexa buffer.

Parameters

Key	Pointer to an array of size 32 which contains AES key in hexa decimal.
-----	--

Returns

Crc of provided AES key value.

Note

This API calculates CRC of AES key for Ultrascale Microblaze's PL eFuse and ZynqMp Ultrascale's PS eFuse. This API calculates CRC on AES key provided in hexa format. To calculate CRC on the AES key in string format please use XilSkey_CrcCalculation. To call this API one can directly pass array of AES key which exists in an instance. Example for storing key into Buffer: If Key is "123456" buffer should be {0x12 0x34 0x56}

User-Configurable Parameters

Overview

This chapter provides detailed descriptions of the various user configurable parameters.

Modules

- [Zynq User-Configurable PS eFUSE Parameters](#)
 - [Zynq User-Configurable PL eFUSE Parameters](#)
 - [Zynq User-Configurable PL BBRAM Parameters](#)
 - [UltraScale or UltraScale+ User-Configurable BBRAM PL Parameters](#)
 - [UltraScale or UltraScale+ User-Configurable PL eFUSE Parameters](#)
 - [Zynq UltraScale+ MPSoC User-Configurable PS eFUSE Parameters](#)
 - [Zynq UltraScale+ MPSoC User-Configurable PS BBRAM Parameters](#)
 - [Zynq UltraScale+ MPSoC User-Configurable PS PUF Parameters](#)
-

Zynq User-Configurable PS eFUSE Parameters

Define the `XSK_EFUSEPS_DRIVER` macro to use the PS eFUSE.

After defining the macro, provide the inputs defined with `XSK_EFUSEPS_DRIVER` to burn the bits in PS eFUSE. If the bit is to be burned, define the macro as `TRUE`; otherwise define the macro as `FALSE`. For details, refer the following table.

Macro Name	Description
XSK_EFUSEPS_ENABLE_WRITE_PROTECT	<p>Default = FALSE.</p> <p>TRUE to burn the write-protect bits in eFUSE array. Write protect has two bits. When either of the bits is burned, it is considered write-protected. So, while burning the write-protected bits, even if one bit is blown, write API returns success. As previously mentioned, POR reset is required after burning for write protection of the eFUSE bits to go into effect. It is recommended to do the POR reset after write protection. Also note that, after write-protect bits are burned, no more eFUSE writes are possible.</p> <p>If the write-protect macro is TRUE with other macros, write protect is burned in the last iteration, after burning all the defined values, so that for any error while burning other macros will not effect the total eFUSE array.</p> <p>FALSE does not modify the write-protect bits.</p>
XSK_EFUSEPS_ENABLE_RSA_AUTH	<p>Default = FALSE.</p> <p>Use TRUE to burn the RSA enable bit in the PS eFUSE array. After enabling the bit, every successive boot must be RSA-enabled apart from JTAG. Before burning (blowing) this bit, make sure that eFUSE array has the valid PPK hash. If the PPK hash burning is enabled, only after writing the hash successfully, RSA enable bit will be blown. For the RSA enable bit to take effect, POR reset is required.</p> <p>FALSE does not modify the RSA enable bit.</p>
XSK_EFUSEPS_ENABLE_ROM_128K_CRC	<p>Default = FALSE.</p> <p>TRUE burns the ROM 128K CRC bit. In every successive boot, BootROM calculates 128k CRC.</p> <p>FALSE does not modify the ROM CRC 128K bit.</p>
XSK_EFUSEPS_ENABLE_RSA_KEY_HASH	<p>Default = FALSE.</p> <p>TRUE burns (blows) the eFUSE hash, that is given in XSK_EFUSEPS_RSA_KEY_HASH_VALUE when write API is used. TRUE reads the eFUSE hash when the read API is used and is read into structure.</p> <p>FALSE ignores the provided value.</p>

Macro Name	Description
XSK_EFUSEPS_RSA_KEY_HASH_VALUE	Default = 00000000000000000000000000000000 The specified value is converted to a hexadecimal buffer and written into the PS eFUSE array when the write API is used. This value should be the Primary Public Key (PPK) hash provided in string format. The buffer must be 64 characters long: valid characters are 0-9, a-f, and A-F. Any other character is considered an invalid string and will not burn RSA hash. When the Xilsky_EfusePs_Write() API is used, the RSA hash is written, and the XSK_EFUSEPS_ENABLE_RSA_KEY_HASH must have a value of TRUE.
XSK_EFUSEPS_DISABLE_DFT_JTAG	Default = FALSE TRUE disables DFT JTAG permanently. FALSE will not modify the eFuse PS DFT JTAG disable bit.
XSK_EFUSEPS_DISABLE_DFT_MODE	Default = FALSE TRUE disables DFT mode permanently. FALSE will not modify the eFuse PS DFT mode disable bit.

Zynq User-Configurable PL eFUSE Parameters

Overview

Define the XSK_EFUSEPL_DRIVER macro to use the PL eFUSE.

After defining the macro, provide the inputs defined with XSK_EFUSEPL_DRIVER to burn the bits in PL eFUSE bits. If the bit is to be burned, define the macro as TRUE; otherwise define the macro as FALSE. The table below lists the user-configurable PL eFUSE parameters for Zynq® devices.

Macro Name	Description
XSK_EFUSEPL_FORCE_PCYCLE_RECONFIG	Default = FALSE If the value is set to TRUE, then the part has to be power-cycled to be reconfigured. FALSE does not set the eFUSE control bit.
XSK_EFUSEPL_DISABLE_KEY_WRITE	Default = FALSE TRUE disables the eFUSE write to FUSE_AES and FUSE_USER blocks. FALSE does not affect the EFUSE bit.

Macro Name	Description
XSK_EFUSEPL_DISABLE_AES_KEY_READ	Default = FALSE TRUE disables the write to FUSE_AES and FUSE_USER key and disables the read of FUSE_AES. FALSE does not affect the eFUSE bit.
XSK_EFUSEPL_DISABLE_USER_KEY_READ	Default = FALSE. TRUE disables the write to FUSE_AES and FUSE_USER key and disables the read of FUSE_USER. FALSE does not affect the eFUSE bit.
XSK_EFUSEPL_DISABLE_FUSE_CNTRL_WRITE	Default = FALSE. TRUE disables the eFUSE write to FUSE_CTRL block. FALSE does not affect the eFUSE bit.
XSK_EFUSEPL_FORCE_USE_AES_ONLY	Default = FALSE. TRUE forces the use of secure boot with eFUSE AES key only. FALSE does not affect the eFUSE bit.
XSK_EFUSEPL_DISABLE_JTAG_CHAIN	Default = FALSE. TRUE permanently disables the Zynq ARM DAP and PL TAP. FALSE does not affect the eFUSE bit.
XSK_EFUSEPL_BBRAM_KEY_DISABLE	Default = FALSE. TRUE forces the eFUSE key to be used if booting Secure Image. FALSE does not affect the eFUSE bit.

Modules

- [MIO Pins for Zynq PL eFUSE JTAG Operations](#)
- [MUX Selection Pin for Zynq PL eFUSE JTAG Operations](#)
- [MUX Parameter for Zynq PL eFUSE JTAG Operations](#)
- [AES and User Key Parameters](#)

MIO Pins for Zynq PL eFUSE JTAG Operations

The table below lists the MIO pins for Zynq PL eFUSE JTAG operations.
You can change the listed pins at your discretion.

Note

The pin numbers listed in the table below are examples. You must assign appropriate pin numbers as per your hardware design.

Pin Name	Pin Number
XSK_EFUSEPL_MIO_JTAG_TDI	(17)
XSK_EFUSEPL_MIO_JTAG_TDO	(18)
XSK_EFUSEPL_MIO_JTAG_TCK	(19)
XSK_EFUSEPL_MIO_JTAG_TMS	(20)

MUX Selection Pin for Zynq PL eFUSE JTAG Operations

The table below lists the MUX selection pin.

Pin Name	Pin Number	Description
XSK_EFUSEPL_MIO_JTAG_MUX_SELECT	(21)	This pin toggles between the external JTAG or MIO driving JTAG operations.

MUX Parameter for Zynq PL eFUSE JTAG Operations

The table below lists the MUX parameter.

Parameter Name	Description
XSK_EFUSEPL_MIO_MUX_SEL_DEFAULT_VAL	Default = LOW. LOW writes zero on the MUX select line before PL_eFUSE writing. HIGH writes one on the MUX select line before PL_eFUSE writing.

The table below lists the AES and user key parameters.

XilSKey Library v6.6
UG1191 (2018.3) November 14, 2018

Parameter Name	Description
XSK_EFUSEPL_USER_HIGH_KEY	<p>Default = 000000</p> <p>The default value is converted to a hexadecimal buffer and written into the PL eFUSE array when the write API is used. This value is the User High Key given in string format. The buffer must be six characters long: valid characters are 0-9, a-f, A-F. Any other character is considered to be an invalid string and does not burn User High Key.</p> <p>To write the User High Key, the XSK_EFUSEPL_PROGRAM_USER_HIGH_KEY must have a value of TRUE.</p>

Zynq User-Configurable PL BBRAM Parameters

Overview

The table below lists the MIO pins for Zynq PL BBRAM JTAG operations.

Note

The pin numbers listed in the table below are examples. You must assign appropriate pin numbers as per your hardware design.

Pin Name	Pin Number
XSK_BBRAM_MIO_JTAG_TDI	(17)
XSK_BBRAM_MIO_JTAG_TDO	(21)
XSK_BBRAM_MIO_JTAG_TCK	(19)
XSK_BBRAM_MIO_JTAG_TMS	(20)

The table below lists the MUX selection pin for Zynq BBRAM PL JTAG operations.

Pin Name	Pin Number
XSK_BBRAM_MIO_JTAG_MUX_SELECT	(11)

Modules

- [MUX Parameter for Zynq BBRAM PL JTAG Operations](#)
- [AES and User Key Parameters](#)

MUX Parameter for Zynq BBRAM PL JTAG Operations

The table below lists the MUX parameter for Zynq BBRAM PL JTAG operations.

Parameter Name	Description
XSK_BBRAM_MIO_MUX_SEL_DEFAULT_VAL	Default = LOW. LOW writes zero on the MUX select line before PL_eFUSE writing. HIGH writes one on the MUX select line before PL_eFUSE writing.

AES and User Key Parameters

The table below lists the AES and user key parameters.

Parameter Name	Description
XSK_BBRAM_AES_KEY	Default = XX. AES key (in HEX) that must be programmed into BBRAM.
XSK_BBRAM_AES_KEY_SIZE_IN_BITS	Default = 256. Size of AES key. Must be 256 bits.

UltraScale or UltraScale+ User-Configurable BBRAM PL Parameters

Overview

Following parameters need to be configured.

Based on your inputs, BBRAM is programmed with the provided AES key.

Modules

- [AES Keys and Related Parameters](#)
- [DPA Protection for BBRAM key](#)
- [GPIO Pins Used for PL Master JTAG and HWM Signals](#)
- [GPIO Channels](#)

AES Keys and Related Parameters

The following table shows AES key related parameters.

Parameter Name	Description
XSK_BBRAM_PGM_OBFUSCATED_KEY	<p>Default = FALSE</p> <p>By default XSK_BBRAM_PGM_OBFUSCATED_KEY is FALSE, BBRAM is programmed with a non-obfuscated key provided in XSK_BBRAM_AES_KEY and DPA protection can be either in enabled/disabled state. TRUE programs the BBRAM with key provided in XSK_BBRAM_OBFUSCATED_KEY and DPA protection cannot be enabled.</p>
XSK_BBRAM_OBFUSCATED_KEY	<p>Default = b1c276899d71fb4cdd4a0a7905ea46c2e11f9574d09c7ea23b70b67de713ccd1</p> <p>The value mentioned in this will be converted to hex buffer and the key is programmed into BBRAM, when program API is called. It should be 64 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not program BBRAM.</p> <p>Note</p> <p>For writing the OBFUSCATED Key, XSK_BBRAM_PGM_OBFUSCATED_KEY should have TRUE value.</p>
XSK_BBRAM_AES_KEY	<p>Default = 00000000000000000524156a63950bcedaf eadcdeabaadee34216615aaaabbbaaa</p> <p>The value mentioned in this will be converted to hex buffer and the key is programmed into BBRAM, when program API is called. It should be 64 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not program BBRAM.</p> <p>Note</p> <p>For programming BBRAM with the key, XSK_BBRAM_PGM_OBFUSCATED_KEY should have a FALSE value.</p>
XSK_BBRAM_AES_KEY_SIZE_IN_BITS	<p>Default= 256</p> <p>Size of AES key must be 256 bits.</p>

DPA Protection for BBRAM key

The following table shows DPA protection configurable parameter.

Parameter Name	Description
XSK_BBRAM_DPA_PROTECT_ENABLE	Default = FALSE By default, the DPA protection will be in disabled state. TRUE will enable DPA protection with provided DPA count and configuration in XSK_BBRAM_DPA_COUNT and XSK_BBRAM_DPA_MODE respectively. DPA protection cannot be enabled if BBRAM is been programmed with an obfuscated key.
XSK_BBRAM_DPA_COUNT	Default = 0 This input is valid only when DPA protection is enabled. Valid range of values are 1 - 255 when DPA protection is enabled else 0.
XSK_BBRAM_DPA_MODE	Default = XSK_BBRAM_INVALID_CONFIGURATIONS When DPA protection is enabled it can be XSK_BBRAM_INVALID_CONFIGURATIONS or XSK_BBRAM_ALL_CONFIGURATIONS If DPA protection is disabled this input provided over here is ignored.

GPIO Pins Used for PL Master JTAG and HWM Signals

In Ultrascale the following GPIO pins are used for connecting MASTER_JTAG pins to access BBRAM. These can be changed depending on your hardware. The table below shows the GPIO pins used for PL MASTER JTAG signals.

Master JTAG Signal	Default PIN Number
XSK_BBRAM_AXI_GPIO_JTAG_TDO	0
XSK_BBRAM_AXI_GPIO_JTAG_TDI	0
XSK_BBRAM_AXI_GPIO_JTAG_TMS	1
XSK_BBRAM_AXI_GPIO_JTAG_TCK	2

GPIO Channels

The following table shows GPIO channel number.

Parameter	Default Channel Number	Master JTAG Signal Connected
XSK_BBRAM_GPIO_INPUT_CH	2	TDO
XSK_BBRAM_GPIO_OUTPUT_CH	1	TDI, TMS, TCK

Note

All inputs and outputs of GPIO can be configured in single channel. For example, XSK_BBRAM_GPIO_INPUT_CH = XSK_BBRAM_GPIO_OUTPUT_CH = 1 or 2. Among (TDI, TCK, TMS) Outputs of GPIO cannot be connected to different GPIO channels all the 3 signals should be in same channel. TDO can be a other channel of (TDI, TCK, TMS) or the same. DPA protection can be enabled only when programming non-obfuscated key.

UltraScale or UltraScale+ User-Configurable PL eFUSE Parameters

Overview

The table below lists the user-configurable PL eFUSE parameters for UltraScale™ devices.

Macro Name	Description
XSK_EFUSEPL_DISABLE_AES_KEY_READ	Default = FALSE TRUE will permanently disable the write to FUSE_AES and check CRC for AES key by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_USER_KEY_READ	Default = FALSE TRUE will permanently disable the write to 32 bit FUSE_USER and read of FUSE_USER key by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_SECURE_READ	Default = FALSE TRUE will permanently disable the write to FUSE_Secure block and reading of secure block by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_FUSE_CNTRL_WRITE	Default = FALSE. TRUE will permanently disable the write to FUSE_CNTRL block by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.

Macro Name	Description
XSK_EFUSEPL_DISABLE_RSA_KEY_READ	Default = FALSE. TRUE will permanently disable the write to FUSE_RSA block and reading of FUSE_RSA Hash by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_KEY_WRITE	Default = FALSE. TRUE will permanently disable the write to FUSE_AES block by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_USER_KEY_WRITE	Default = FALSE. TRUE will permanently disable the write to FUSE_USER block by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_SECURE_WRITE	Default = FALSE. TRUE will permanently disable the write to FUSE_SECURE block by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_RSA_HASH_WRITE	Default = FALSE. TRUE will permanently disable the write to FUSE_RSA authentication key by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_DISABLE_128BIT_USER_KEY_WRITE	Default = FALSE. TRUE will permanently disable the write to 128 bit FUSE_USER by programming control bit of FUSE. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPL_ALLOW_ENCRYPTED_ONLY	Default = FALSE. TRUE will permanently allow encrypted bitstream only. FALSE will not modify this Secure bit of eFuse.
XSK_EFUSEPL_FORCE_USE_FUSE_AES_ONLY	Default = FALSE. TRUE then allows only FUSE's AES key as source of encryption FALSE then allows FPGA to configure an unencrypted bitstream or bitstream encrypted using key stored BBRAM or eFuse.
XSK_EFUSEPL_ENABLE_RSA_AUTH	Default = FALSE. TRUE will enable RSA authentication of bitstream FALSE will not modify this secure bit of eFuse.

Macro Name	Description
XSK_EFUSEPL_DISABLE_JTAG_CHAIN	Default = FALSE. TRUE will disable JTAG permanently. FALSE will not modify this secure bit of eFuse.
XSK_EFUSEPL_DISABLE_TEST_ACCESS	Default = FALSE. TRUE will disables Xilinx test access. FALSE will not modify this secure bit of eFuse.
XSK_EFUSEPL_DISABLE_AES_DECRYPTOR	Default = FALSE. TRUE will disables decoder completely. FALSE will not modify this secure bit of eFuse.
XSK_EFUSEPL_ENABLE_OBFUSCATION_EFUSEAES	Default = FALSE. TRUE will enable obfuscation feature for eFUSE AES key.

Modules

- [GPIO Pins Used for PL Master JTAG Signal](#)
- [GPIO Channels](#)
- [AES Keys and Related Parameters](#)

GPIO Pins Used for PL Master JTAG Signal

In Ultrascale the following GPIO pins are used for connecting MASTER_JTAG pins to access BBRAM. These can be changed depending on your hardware. The table below shows the GPIO pins used for PL MASTER JTAG signals.

Master JTAG Signal	Default PIN Number
XSK_EFUSEPL_AXI_GPIO_JTAG_TDO	0
XSK_EFUSEPL_AXI_GPIO_HWM_READY	0
XSK_EFUSEPL_AXI_GPIO_HWM_END	1
XSK_EFUSEPL_AXI_GPIO_JTAG_TDI	2
XSK_EFUSEPL_AXI_GPIO_JTAG_TMS	1
XSK_EFUSEPL_AXI_GPIO_JTAG_TCK	2
XSK_EFUSEPL_AXI_GPIO_HWM_START	3

GPIO Channels

The following table shows GPIO channel number.

Parameter	Default Channel Number	Master JTAG Signal Connected
XSK_EFUSEPL_GPIO_INPUT_CH	2	TDO
XSK_EFUSEPL_GPIO_OUTPUT_CH	1	TDI, TMS, TCK

Note

All inputs and outputs of GPIO can be configured in single channel. For example, XSK_BBRAM_GPIO_INPUT_CH = XSK_BBRAM_GPIO_OUTPUT_CH = 1 or 2. Among (TDI, TCK, TMS) Outputs of GPIO cannot be connected to different GPIO channels all the 3 signals should be in same channel. TDO can be a other channel of (TDI, TCK, TMS) or the same. DPA protection can be enabled only when programming non-obfuscated key.

AES Keys and Related Parameters

The following table shows AES key related parameters.

Parameter Name	Description
XSK_EFUSEPL_PROGRAM_AES_KEY_ULTRA	Default = FALSE TRUE will burn the AES key given in XSK_EFUSEPL_AES_KEY. FALSE will ignore the values given.
XSK_EFUSEPL_PROGRAM_USER_KEY_ULTRA	Default = FALSE TRUE will burn 32 bit User key given in XSK_EFUSEPL_USER_KEY. FALSE will ignore the values given.
XSK_EFUSEPL_PROGRAM_RSA_HASH_ULTRA	Default = FALSE TRUE will burn RSA hash given in XSK_EFUSEPL_RSA_KEY_HASH_VALUE. FALSE will ignore the values given.
XSK_EFUSEPL_PROGRAM_USER_KEY_128BIT	Default = FALSE TRUE will burn 128 bit User key given in XSK_EFUSEPL_USER_KEY_128BIT_0, XSK_EFUSEPL_USER_KEY_128BIT_1, XSK_EFUSEPL_USER_KEY_128BIT_2, XSK_EFUSEPL_USER_KEY_128BIT_3 FALSE will ignore the values given.

[Send Feedback](#)

Zynq UltraScale+ MPSoC User-Configurable PS eFUSE Parameters

Overview

The table below lists the user-configurable PS eFUSE parameters for Zynq UltraScale+ MPSoC devices.

Macro Name	Description
XSK_EFUSEPS_AES_RD_LOCK	Default = FALSE TRUE will permanently disable the CRC check of FUSE_AES. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_AES_WR_LOCK	Default = FALSE TRUE will permanently disable the writing to FUSE_AES block. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_ENC_ONLY	Default = FALSE TRUE will permanently enable encrypted booting only using the Fuse key. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_BBRAM_DISABLE	Default = FALSE TRUE will permanently disable the BBRAM key. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_ERR_DISABLE	Default = FALSE TRUE will permanently disables the error messages in JTAG status register. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_JTAG_DISABLE	Default = FALSE TRUE will permanently disable JTAG controller. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_DFT_DISABLE	Default = FALSE TRUE will permanently disable DFT boot mode. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_PROG_GATE_DISABLE	Default = FALSE TRUE will permanently disable PROG_GATE feature in PPD. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_SECURE_LOCK	Default = FALSE TRUE will permanently disable reboot into JTAG mode when doing a secure lockdown. FALSE will not modify this control bit of eFuse.

Macro Name	Description
XSK_EFUSEPS_RSA_ENABLE	Default = FALSE TRUE will permanently enable RSA authentication during boot. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_PPK0_WR_LOCK	Default = FALSE TRUE will permanently disable writing to PPK0 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_PPK0_INVLD	Default = FALSE TRUE will permanently revoke PPK0. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_PPK1_WR_LOCK	Default = FALSE TRUE will permanently disable writing PPK1 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_PPK1_INVLD	Default = FALSE TRUE will permanently revoke PPK1. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_0	Default = FALSE TRUE will permanently disable writing to USER_0 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_1	Default = FALSE TRUE will permanently disable writing to USER_1 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_2	Default = FALSE TRUE will permanently disable writing to USER_2 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_3	Default = FALSE TRUE will permanently disable writing to USER_3 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_4	Default = FALSE TRUE will permanently disable writing to USER_4 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_5	Default = FALSE TRUE will permanently disable writing to USER_5 efuses. FALSE will not modify this control bit of eFuse.

Macro Name	Description
XSK_EFUSEPS_USER_WRLK_6	Default = FALSE TRUE will permanently disable writing to USER_6 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_USER_WRLK_7	Default = FALSE TRUE will permanently disable writing to USER_7 efuses. FALSE will not modify this control bit of eFuse.
XSK_EFUSEPS_LBIST_EN	Default = FALSE TRUE will permanently enables logic BIST to be run during boot. FALSE will not modify this control bit of eFUSE.
XSK_EFUSEPS_LPD_SC_EN	Default = FALSE TRUE will permanently enables zeroization of registers in Low Power Domain(LPD) during boot. FALSE will not modify this control bit of eFUSE.
XSK_EFUSEPS_FPD_SC_EN	Default = FALSE TRUE will permanently enables zeroization of registers in Full Power Domain(FPD) during boot. FALSE will not modify this control bit of eFUSE.
XSK_EFUSEPS_PBR_BOOT_ERR	Default = FALSE TRUE will permanently enables the boot halt when there is any PMU error. FALSE will not modify this control bit of eFUSE.

Modules

- [AES Keys and Related Parameters](#)
- [User Keys and Related Parameters](#)
- [PPK0 Keys and Related Parameters](#)
- [PPK1 Keys and Related Parameters](#)
- [SPK ID and Related Parameters](#)

AES Keys and Related Parameters

The following table shows AES key related parameters.

Parameter Name	Description
XSK_EFUSEPS_WRITE_AES_KEY	Default = TRUE TRUE will burn the AES key provided in XSK_EFUSEPS_AES_KEY. FALSE will ignore the key provide XSK_EFUSEPS_AES_KEY.

Parameter Name	Description
XSK_EFUSEPS_AES_KEY	<p>Default = 00000000000000000000000000000000 00000000000000000000000000000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 64 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn AES Key.</p> <p>Note</p> <p>For writing the AES Key, XSK_EFUSEPS_WRITE_AES_KEY should have TRUE value.</p>

User Keys and Related Parameters

Single bit programming is allowed for all the USER fuses.

If user requests to revert already programmed bit. Library throws an error. If user fuses is non-zero also library will not throw an error for valid requests The following table shows the user keys and related parameters.

Parameter Name	Description
XSK_EFUSEPS_WRITE_USER0_FUSE	Default = TRUE TRUE will burn User0 Fuse provided in XSK_EFUSEPS_USER0_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER0_FUSES
XSK_EFUSEPS_WRITE_USER1_FUSE	Default = TRUE TRUE will burn User1 Fuse provided in XSK_EFUSEPS_USER1_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER1_FUSES
XSK_EFUSEPS_WRITE_USER2_FUSE	Default = TRUE TRUE will burn User2 Fuse provided in XSK_EFUSEPS_USER2_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER2_FUSES
XSK_EFUSEPS_WRITE_USER3_FUSE	Default = TRUE TRUE will burn User3 Fuse provided in XSK_EFUSEPS_USER3_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER3_FUSES

Parameter Name	Description
XSK_EFUSEPS_WRITE_USER4_FUSE	Default = TRUE TRUE will burn User4 Fuse provided in XSK_EFUSEPS_USER4_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER4_FUSES
XSK_EFUSEPS_WRITE_USER5_FUSE	Default = TRUE TRUE will burn User5 Fuse provided in XSK_EFUSEPS_USER5_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER5_FUSES
XSK_EFUSEPS_WRITE_USER6_FUSE	Default = TRUE TRUE will burn User6 Fuse provided in XSK_EFUSEPS_USER6_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER6_FUSES
XSK_EFUSEPS_WRITE_USER7_FUSE	Default = TRUE TRUE will burn User7 Fuse provided in XSK_EFUSEPS_USER7_FUSES. FALSE will ignore the value provided in XSK_EFUSEPS_USER7_FUSES
XSK_EFUSEPS_USER0_FUSES	Default = 00000000 The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID. Note For writing the User0 Fuse, XSK_EFUSEPS_WRITE_USER0_FUSE should have TRUE value

Parameter Name	Description
XSK_EFUSEPS_USER1_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User1 Fuse, XSK_EFUSEPS_WRITE_USER1_FUSE should have TRUE value</p>
XSK_EFUSEPS_USER2_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User2 Fuse, XSK_EFUSEPS_WRITE_USER2_FUSE should have TRUE value</p>
XSK_EFUSEPS_USER3_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User3 Fuse, XSK_EFUSEPS_WRITE_USER3_FUSE should have TRUE value</p>

Parameter Name	Description
XSK_EFUSEPS_USER4_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User4 Fuse, XSK_EFUSEPS_WRITE_USER4_FUSE should have TRUE value</p>
XSK_EFUSEPS_USER5_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User5 Fuse, XSK_EFUSEPS_WRITE_USER5_FUSE should have TRUE value</p>
XSK_EFUSEPS_USER6_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User6 Fuse, XSK_EFUSEPS_WRITE_USER6_FUSE should have TRUE value</p>

Parameter Name	Description
XSK_EFUSEPS_USER7_FUSES	<p>Default = 00000000</p> <p>The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the User7 Fuse, XSK_EFUSEPS_WRITE_USER7_FUSE should have TRUE value</p>

PPK0 Keys and Related Parameters

The following table shows the PPK0 keys and related parameters.

Parameter Name	Description
XSK_EFUSEPS_WRITE_PPK0_SHA3_HASH	<p>Default = TRUE</p> <p>TRUE will burn PPK0 sha3 hash provided in XSK_EFUSEPS_PPK0_SHA3_HASH. FALSE will ignore the hash provided in XSK_EFUSEPS_PPK0_SHA3_HASH.</p>
XSK_EFUSEPS_PPK0_IS_SHA3	<p>Default = TRUE</p> <p>TRUE XSK_EFUSEPS_PPK0_SHA3_HASH should be of string length 96 it specifies that PPK0 is used to program SHA3 hash. FALSE XSK_EFUSEPS_PPK0_SHA3_HASH should be of string length 64 it specifies that PPK0 is used to program SHA2 hash.</p>

PPK1 Keys and Related Parameters

Parameter Name	Description
XSK_EFUSEPS_WRITE_PPK1_SHA3_HASH	Default = TRUE TRUE will burn PPK1 sha3 hash provided in XSK_EFUSEPS_PPK1_SHA3_HASH. FALSE will ignore the hash provided in XSK_EFUSEPS_PPK1_SHA3_HASH.
XSK_EFUSEPS_PPK1_IS_SHA3	Default = FALSE TRUE XSK_EFUSEPS_PPK1_SHA3_HASH should be of string length 96 it specifies that PPK1 is used to program SHA3 hash. FALSE XSK_EFUSEPS_PPK1_SHA3_HASH should be of string length 64 it specifies that PPK1 is used to program SHA2 hash.

SPK ID and Related Parameters

Parameter Name	Description
XSK_EFUSEPS_WRITE_SPKID	<p>Default = TRUE TRUE will burn SPKID provided in XSK_EFUSEPS_SPK_ID. FALSE will ignore the hash provided in XSK_EFUSEPS_SPK_ID.</p>
XSK_EFUSEPS_SPK_ID	<p>Default = 00000000 The value mentioned in this will be converted to hex buffer and written into the Zynq UltraScale+ MPSoC PS eFUSE array when write API used. This value should be given in string format. It should be 8 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string and will not burn SPK ID.</p> <p>Note</p> <p>For writing the SPK ID, XSK_EFUSEPS_WRITE_SPKID should have TRUE value.</p>

Note

PPK hash should be unmodified hash generated by bootgen. Single bit programming is allowed for User FUSEs (0 to 7), if you specify a value that tries to set a bit that was previously programmed to 1 back to 0, you will get an error. you have to provide already programmed bits also along with new requests.

Zynq	UltraScale+	MPSoC	User-Configurable	PS
BBRAM Parameters				

The table below lists the AES and user key parameters.

Parameter Name	Description
XSK_ZYNQMP_BBRAMPS_AES_KEY	Default = 00000000000000000000000000000000 00000000000000000000000000000000 AES key (in HEX) that must be programmed into BBRAM.
XSK_ZYNQMP_BBRAMPS_AES_KEY_LEN_IN_BYTES	Default = 32. Length of AES key in bytes.
XSK_ZYNQMP_BBRAMPS_AES_KEY_LEN_IN_BITS	Default = 256. Length of AES key in bits.
XSK_ZYNQMP_BBRAMPS_AES_KEY_STR_LEN	Default = 64. String length of the AES key.

Zynq UltraScale+ MPSoC User-Configurable PS PUF Parameters

The table below lists the user-configurable PS PUF parameters for Zynq UltraScale+ MPSoC devices.

Macro Name	Description
XSK_PUF_INFO_ON_UART	Default = FALSE TRUE will display syndrome data on UART com port FALSE will display any data on UART com port.
XSK_PUF_PROGRAM_EFUSE	Default = FALSE TRUE will program the generated syndrome data, CHash and Auxilary values, Black key. FALSE will not program data into eFUSE.
XSK_PUF_IF_CONTRACT_MANUFACTURER	Default = FALSE This should be enabled when application is hand over to contract manufacturer. TRUE will allow only authenticated application. FALSE authentication is not mandatory.
XSK_PUF_REG_MODE	Default = XSK_PUF_MODE4K PUF registration is performed in 4K mode. For only understanding it is provided in this file, but user is not supposed to modify this.

[illegible]

Macro Name	Description
XSK_PUF_BLACK_KEY_IV	<p>Default = 000000000000000000000000</p> <p>The value mentioned here will be converted to hex buffer. This is Initialization vector(IV) which is used to generated black key with provided AES key and generated PUF key.</p> <p>This value should be given in string format. It should be 24 characters long, valid characters are 0-9,a-f,A-F. Any other character is considered as invalid string.</p>

Error Codes

Overview

The application error code is 32 bits long.
For example, if the error code for PS is 0x8A05:

- 0x8A indicates that a write error has occurred while writing RSA Authentication bit.
- 0x05 indicates that write error is due to the write temperature out of range.

Applications have the following options on how to show error status. Both of these methods of conveying the status are implemented by default. However, UART is required to be present and initialized for status to be displayed through UART.

- Send the error code through UART pins
- Write the error code in the reboot status register

Modules

- [PL eFUSE Error Codes](#)
- [PS eFUSE Error Codes](#)
- [Zynq UltraScale+ MPSoC BBRAM PS Error Codes](#)

PL eFUSE Error Codes

`XSK_EFUSEPL_ERROR_NONE` 0
No error.

`XSK_EFUSEPL_ERROR_ROW_NOT_ZERO` 0x10
Row is not zero.

`XSK_EFUSEPL_ERROR_READ_ROW_OUT_OF_RANGE` 0x11
Read Row is out of range.

`XSK_EFUSEPL_ERROR_READ_MARGIN_OUT_OF_RANGE` 0x12
Read Margin is out of range.

`XSK_EFUSEPL_ERROR_READ_BUFFER_NULL` 0x13
No buffer for read.

XSK_EFUSEPL_ERROR_READ_BIT_VALUE_NOT_SET	0x14
Read bit not set.	
XSK_EFUSEPL_ERROR_READ_BIT_OUT_OF_RANGE	<0x15 br>Read bit is out of range.
XSK_EFUSEPL_ERROR_READ_TEMPERATURE_OUT_OF_RANGE	0x16
Temperature obtained from XADC is out of range to read.	
XSK_EFUSEPL_ERROR_READ_VCCAUX_VOLTAGE_OUT_OF_RANGE	0x17
VCCAUX obtained from XADC is out of range to read.	
XSK_EFUSEPL_ERROR_READ_VCCINT_VOLTAGE_OUT_OF_RANGE	0x18
VCCINT obtained from XADC is out of range to read.	
XSK_EFUSEPL_ERROR_WRITE_ROW_OUT_OF_RANGE	0x19
To write row is out of range.	
XSK_EFUSEPL_ERROR_WRITE_BIT_OUT_OF_RANGE	0x1A
To read bit is out of range.	
XSK_EFUSEPL_ERROR_WRITE_TEMPERATURE_OUT_OF_RANGE	0x1B
To eFUSE write Temperature obtained from XADC is out of range.	
XSK_EFUSEPL_ERROR_WRITE_VCCAUX_VOLTAGE_OUT_OF_RANGE	0x1C
To write eFUSE VCCAUX obtained from XADC is out of range.	
XSK_EFUSEPL_ERROR_WRITE_VCCINT_VOLTAGE_OUT_OF_RANGE	0x1D
To write into eFUSE VCCINT obtained from XADC is out of range.	
XSK_EFUSEPL_ERROR_FUSE_CNTRL_WRITE_DISABLED	0x1E
Fuse control write is disabled.	
XSK_EFUSEPL_ERROR_CNTRL_WRITE_BUFFER_NULL	0x1F
Buffer pointer that is supposed to contain control data is null.	
XSK_EFUSEPL_ERROR_NOT_VALID_KEY_LENGTH	0x20
Key length invalid.	
XSK_EFUSEPL_ERROR_ZERO_KEY_LENGTH	0x21
Key length zero.	
XSK_EFUSEPL_ERROR_NOT_VALID_KEY_CHAR	0x22
Invalid key characters.	
XSK_EFUSEPL_ERROR_NULL_KEY	0x23
Null key.	
XSK_EFUSEPL_ERROR_FUSE_SEC_WRITE_DISABLED	0x24
Secure bits write is disabled.	
XSK_EFUSEPL_ERROR_FUSE_SEC_READ_DISABLED	0x25
Secure bits reading is disabled.	
XSK_EFUSEPL_ERROR_SEC_WRITE_BUFFER_NULL	0x26
Buffer to write into secure block is NULL.	
XSK_EFUSEPL_ERROR_READ_PAGE_OUT_OF_RANGE	0x27
Page is out of range.	
XSK_EFUSEPL_ERROR_FUSE_ROW_RANGE	0x28
Row is out of range.	
XSK_EFUSEPL_ERROR_IN_PROGRAMMING_ROW	0x29
Error programming fuse row.	

XSK_EFUSEPL_ERROR_PRGRMG_ROWS_NOT_EMPTY	0x2A
Error when tried to program non Zero rows of eFUSE.	
XSK_EFUSEPL_ERROR_HWM_TIMEOUT	0x80
Error when hardware module is exceeded the time for programming eFUSE.	
XSK_EFUSEPL_ERROR_USER_FUSE_REVERT	0x90
Error occurs when user requests to revert already programmed user eFUSE bit.	
XSK_EFUSEPL_ERROR_KEY_VALIDATION	0xF000
Invalid key.	
XSK_EFUSEPL_ERROR_PL_STRUCT_NULL	0x1000
Null PL structure.	
XSK_EFUSEPL_ERROR_JTAG_SERVER_INIT	0x1100
JTAG server initialization error.	
XSK_EFUSEPL_ERROR_READING_FUSE_CNTRL	0x1200
Error reading fuse control.	
XSK_EFUSEPL_ERROR_DATA_PROGRAMMING_NOT_ALLOWED	0x1300
Data programming not allowed.	
XSK_EFUSEPL_ERROR_FUSE_CTRL_WRITE_NOT_ALLOWED	0x1400
Fuse control write is disabled.	
XSK_EFUSEPL_ERROR_READING_FUSE_AES_ROW	0x1500
Error reading fuse AES row.	
XSK_EFUSEPL_ERROR_AES_ROW_NOT_EMPTY	0x1600
AES row is not empty.	
XSK_EFUSEPL_ERROR_PROGRAMMING_FUSE_AES_ROW	0x1700
Error programming fuse AES row.	
XSK_EFUSEPL_ERROR_READING_FUSE_USER_DATA_ROW	0x1800
Error reading fuse user row.	
XSK_EFUSEPL_ERROR_USER_DATA_ROW_NOT_EMPTY	0x1900
User row is not empty.	
XSK_EFUSEPL_ERROR_PROGRAMMING_FUSE_DATA_ROW	0x1A00
Error programming fuse user row.	
XSK_EFUSEPL_ERROR_PROGRAMMING_FUSE_CNTRL_ROW	0x1B00
Error programming fuse control row.	
XSK_EFUSEPL_ERROR_XADC	0x1C00
XADC error.	
XSK_EFUSEPL_ERROR_INVALID_REF_CLK	0x3000
Invalid reference clock.	
XSK_EFUSEPL_ERROR_FUSE_SEC_WRITE_NOT_ALLOWED	0x1D00
Error in programming secure block.	
XSK_EFUSEPL_ERROR_READING_FUSE_STATUS	0x1E00
Error in reading FUSE status.	
XSK_EFUSEPL_ERROR_FUSE_BUSY	0x1F00
Fuse busy.	

XSK_EFUSEPL_ERROR_READING_FUSE_RSA_ROW 0x2000

Error in reading FUSE RSA block.

XSK_EFUSEPL_ERROR_TIMER_INTIALISE_ULTRA 0x2200

Error in initiating Timer.

XSK_EFUSEPL_ERROR_READING_FUSE_SEC 0x2300

Error in reading FUSE secure bits.

XSK_EFUSEPL_ERROR_PRGRMG_FUSE_SEC_ROW 0x2500

Error in programming Secure bits of efuse.

XSK_EFUSEPL_ERROR_PRGRMG_USER_KEY 0x4000

Error in programming 32 bit user key.

XSK_EFUSEPL_ERROR_PRGRMG_128BIT_USER_KEY 0x5000

Error in programming 128 bit User key.

XSK_EFUSEPL_ERROR_PRGRMG_RSA_HASH 0x8000

Error in programming RSA hash.

PS eFUSE Error Codes

XSK_EFUSEPS_ERROR_NONE 0

No error.

XSK_EFUSEPS_ERROR_ADDRESS_XIL_RESTRICTED 0x01

Address is restricted.

XSK_EFUSEPS_ERROR_READ_TMEPERATURE_OUT_OF_RANGE 0x02

Temperature obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_READ_VCCPAUX_VOLTAGE_OUT_OF_RANGE 0x03

VCCAUX obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_READ_VCCPINT_VOLTAGE_OUT_OF_RANGE 0x04

VCCINT obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_WRITE_TEMPERATURE_OUT_OF_RANGE 0x05

Temperature obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_WRITE_VCCPAUX_VOLTAGE_OUT_OF_RANGE 0x06

VCCAUX obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_WRITE_VCCPINT_VOLTAGE_OUT_OF_RANGE 0x07

VCCINT obtained from XADC is out of range.

XSK_EFUSEPS_ERROR_VERIFICATION 0x08

Verification error.

XSK_EFUSEPS_ERROR_RSA_HASH_ALREADY_PROGRAMMED 0x09

RSA hash was already programmed.

XSK_EFUSEPS_ERROR_CONTROLLER_MODE 0x0A

Controller mode error

XSK_EFUSEPS_ERROR_REF_CLOCK 0x0B

Reference clock not between 20 to 60MHz

XSK_EFUSEPS_ERROR_READ_MODE 0x0C

Not supported read mode

XSK_EFUSEPS_ERROR_XADC_CONFIG	0x0D	XADC configuration error.
XSK_EFUSEPS_ERROR_XADC_INITIALIZE	0x0E	XADC initialization error.
XSK_EFUSEPS_ERROR_XADC_SELF_TEST	0x0F	XADC self-test failed.
XSK_EFUSEPS_ERROR_PARAMETER_NULL	Utils Error Codes. 0x10	Passed parameter null.
XSK_EFUSEPS_ERROR_STRING_INVALID	0x20	Passed string is invalid.
XSK_EFUSEPS_ERROR_AES_ALREADY_PROGRAMMED	0x12	AES key is already programmed.
XSK_EFUSEPS_ERROR_SPKID_ALREADY_PROGRAMMED	0x13	SPK ID is already programmed.
XSK_EFUSEPS_ERROR_PPK0_HASH_ALREADY_PROGRAMMED	0x14	PPK0 hash is already programmed.
XSK_EFUSEPS_ERROR_PPK1_HASH_ALREADY_PROGRAMMED	0x15	PPK1 hash is already programmed.
XSK_EFUSEPS_ERROR_PROGRAMMING_TBIT_PATTERN	0x16	Error in programming TBITS.
XSK_EFUSEPS_ERROR_BEFORE_PROGRAMMING	0x0080	Error occurred before programming.
XSK_EFUSEPS_ERROR_PROGRAMMING	0x00A0	Error in programming eFUSE.
XSK_EFUSEPS_ERROR_READ	0x00B0	Error in reading.
XSK_EFUSEPS_ERROR_BYTES_REQUEST	0x00C0	Error in requested byte count.
XSK_EFUSEPS_ERROR_RESRVD_BITS_PRGRMG	0x00D0	Error in programming reserved bits.
XSK_EFUSEPS_ERROR_ADDR_ACCESS	0x00E0	Error in accessing requested address.
XSK_EFUSEPS_ERROR_PS_STRUCT_NULL	XSKEfuse_Write/Read()common error codes. 0x8100	PS structure pointer is null.
XSK_EFUSEPS_ERROR_XADC_INIT	0x8200	XADC initialization error.
XSK_EFUSEPS_ERROR_CONTROLLER_LOCK	0x8300	PS eFUSE controller is locked.
XSK_EFUSEPS_ERROR_EFUSE_WRITE_PROTECTED	0x8400	PS eFUSE is write protected.
XSK_EFUSEPS_ERROR_CONTROLLER_CONFIG	0x8500	Controller configuration error.

<i>XSK_EFUSEPS_ERROR_PS_PARAMETER_WRONG</i>	0x8600
PS eFUSE parameter is not TRUE/FALSE.	
<i>XSK_EFUSEPS_ERROR_WRITE_128K_CRC_BIT</i>	0x9100
Error in enabling 128K CRC.	
<i>XSK_EFUSEPS_ERROR_WRITE_NONSECURE_INITB_BIT</i>	0x9200
Error in programming NON secure bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_UART_STATUS_BIT</i>	0x9300
Error in writing UART status bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_RSA_HASH</i>	0x9400
Error in writing RSA key.	
<i>XSK_EFUSEPS_ERROR_WRITE_RSA_AUTH_BIT</i>	0x9500
Error in enabling RSA authentication bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_WRITE_PROTECT_BIT</i>	0x9600
Error in writing write-protect bit.	
<i>XSK_EFUSEPS_ERROR_READ_HASH_BEFORE_PROGRAMMING</i>	0x9700
Check RSA key before trying to program.	
<i>XSK_EFUSEPS_ERROR_WRTIE_DFT_JTAG_DIS_BIT</i>	0x9800
Error in programming DFT JTAG disable bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_DFT_MODE_DIS_BIT</i>	0x9900
Error in programming DFT MODE disable bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_AES_CRC_LK_BIT</i>	0x9A00
Error in enabling AES's CRC check lock.	
<i>XSK_EFUSEPS_ERROR_WRTIE_AES_WR_LK_BIT</i>	0x9B00
Error in programming AES write lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USE_AESONLY_EN_BIT</i>	0x9C00
Error in programming use AES only bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_BBRAM_DIS_BIT</i>	0x9D00
Error in programming BBRAM disable bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PMU_ERR_DIS_BIT</i>	0x9E00
Error in programming PMU error disable bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_JTAG_DIS_BIT</i>	0x9F00
Error in programming JTAG disable bit.	
<i>XSK_EFUSEPS_ERROR_READ_RSA_HASH</i>	0xA100
Error in reading RSA key.	
<i>XSK_EFUSEPS_ERROR_WRONG_TBIT_PATTERN</i>	0xA200
Error in programming TBIT pattern.	
<i>XSK_EFUSEPS_ERROR_WRITE_AES_KEY</i>	0xA300
Error in programming AES key.	
<i>XSK_EFUSEPS_ERROR_WRITE_SPK_ID</i>	0xA400
Error in programming SPK ID.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER_KEY</i>	0xA500
Error in programming USER key.	

<i>XSK_EFUSEPS_ERROR_WRITE_PPK0_HASH</i>	<i>0xA600</i>
Error in programming PPK0 hash.	
<i>XSK_EFUSEPS_ERROR_WRITE_PPK1_HASH</i>	<i>0xA700</i>
Error in programming PPK1 hash.	
<i>XSK_EFUSEPS_ERROR_CACHE_LOAD</i>	<i>0xB000</i>
Error in re-loading CACHE.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER0_FUSE</i>	<i>0xC000</i>
Error in programming USER 0 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER1_FUSE</i>	<i>0xC100</i>
Error in programming USER 1 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER2_FUSE</i>	<i>0xC200</i>
Error in programming USER 2 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER3_FUSE</i>	<i>0xC300</i>
Error in programming USER 3 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER4_FUSE</i>	<i>0xC400</i>
Error in programming USER 4 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER5_FUSE</i>	<i>0xC500</i>
Error in programming USER 5 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER6_FUSE</i>	<i>0xC600</i>
Error in programming USER 6 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRITE_USER7_FUSE</i>	<i>0xC700</i>
Error in programming USER 7 Fuses.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER0_LK_BIT</i>	<i>0xC800</i>
Error in programming USER 0 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER1_LK_BIT</i>	<i>0xC900</i>
Error in programming USER 1 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER2_LK_BIT</i>	<i>0xCA00</i>
Error in programming USER 2 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER3_LK_BIT</i>	<i>0xCB00</i>
Error in programming USER 3 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER4_LK_BIT</i>	<i>0xCC00</i>
Error in programming USER 4 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER5_LK_BIT</i>	<i>0xCD00</i>
Error in programming USER 5 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER6_LK_BIT</i>	<i>0xCE00</i>
Error in programming USER 6 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_USER7_LK_BIT</i>	<i>0xCF00</i>
Error in programming USER 7 fuses lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PROG_GATE0_DIS_BIT</i>	<i>0xD000</i>
Error in programming PROG_GATE0 disabling bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PROG_GATE1_DIS_BIT</i>	<i>0xD100</i>
Error in programming PROG_GATE1 disabling bit.	

<i>XSK_EFUSEPS_ERROR_WRTIE_PROG_GATE2_DIS_BIT</i>	<i>0xD200</i>
Error in programming PROG_GATE2 disabling bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_SEC_LOCK_BIT</i>	<i>0xD300</i>
Error in programming SEC_LOCK bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PPK0_WR_LK_BIT</i>	<i>0xD400</i>
Error in programming PPK0 write lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PPK0_RVK_BIT</i>	<i>0xD500</i>
Error in programming PPK0 revoke bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PPK1_WR_LK_BIT</i>	<i>0xD600</i>
Error in programming PPK1 write lock bit.	
<i>XSK_EFUSEPS_ERROR_WRTIE_PPK1_RVK_BIT</i>	<i>0xD700</i>
Error in programming PPK0 revoke bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_PUF_SYN_INVLD</i>	<i>0xD800</i>
Error while programming the PUF syndrome invalidate bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_PUF_SYN_WRLK</i>	<i>0xD900</i>
Error while programming Syndrome write lock bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_PUF_SYN_REG_DIS</i>	<i>0xDA00</i>
Error while programming PUF syndrome register disable bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_PUF_RESERVED_BIT</i>	<i>0xDB00</i>
Error while programming PUF reserved bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_LBIST_EN_BIT</i>	<i>0xDC00</i>
Error while programming LBIST enable bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_LPD_SC_EN_BIT</i>	<i>0xDD00</i>
Error while programming LPD SC enable bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_FPD_SC_EN_BIT</i>	<i>0xDE00</i>
Error while programming FPD SC enable bit.	
<i>XSK_EFUSEPS_ERROR_WRITE_PBR_BOOT_ERR_BIT</i>	<i>0xDF00</i>
Error while programming PBR boot error bit.	
<i>XSK_EFUSEPS_ERROR_PUF_INVALID_REG_MODE</i>	<i>0xE000</i>
Error when PUF registration is requested with invalid registration mode.	
<i>XSK_EFUSEPS_ERROR_PUF_REG_WO_AUTH</i>	<i>0xE100</i>
Error when write not allowed without authentication enabled.	
<i>XSK_EFUSEPS_ERROR_PUF_REG_DISABLED</i>	<i>0xE200</i>
Error when trying to do PUF registration and when PUF registration is disabled.	
<i>XSK_EFUSEPS_ERROR_PUF_INVALID_REQUEST</i>	<i>0xE300</i>
Error when an invalid mode is requested.	
<i>XSK_EFUSEPS_ERROR_PUF_DATA_ALREADY_PROGRAMMED</i>	<i>0xE400</i>
Error when PUF is already programmed in eFUSE.	
<i>XSK_EFUSEPS_ERROR_PUF_DATA_OVERFLOW</i>	<i>0xE500</i>
Error when an over flow occurs.	
<i>XSK_EFUSEPS_ERROR_CMPLTD_EFUSE_PRGRM_WITH_ERR</i>	<i>0x10000</i>
eFUSE programming is completed with temp and vol read errors.	

XSK_EFUSEPS_ERROR_FUSE_PROTECTED 0x00080000

Requested eFUSE is write protected.

XSK_EFUSEPS_ERROR_USER_BIT_CANT_REVERT 0x00800000

Already programmed user FUSE bit cannot be reverted.

Zynq UltraScale+ MPSoC BBRAM PS Error Codes

XSK_ZYNQMP_BBRAMPS_ERROR_NONE 0

No error.

XSK_ZYNQMP_BBRAMPS_ERROR_IN_PRGRMG_ENABLE 0x01

If this error is occurred programming is not possible.

XSK_ZYNQMP_BBRAMPS_ERROR_IN_CRC_CHECK 0xB000

If this error is occurred programming is done but CRC check is failed.

XSK_ZYNQMP_BBRAMPS_ERROR_IN_PRGRMG 0xC000

programming of key is failed.

Status Codes

For Zynq® and UltraScale™, the status in the `xilsky_efuse_example.c` file is conveyed through a UART or reboot status register in the following format: `0xYYYYZZZZ`, where:

- `YYYY` represents the PS eFUSE Status.
- `ZZZZ` represents the PL eFUSE Status.

The table below lists the status codes.

Status Code Values	Description
<code>0x0000ZZZZ</code>	Represents PS eFUSE is successful and PL eFUSE process returned with error.
<code>0xYYYY0000</code>	Represents PL eFUSE is successful and PS eFUSE process returned with error.
<code>0xFFFF0000</code>	Represents PS eFUSE is not initiated and PL eFUSE is successful.
<code>0x0000FFFF</code>	Represents PL eFUSE is not initiated and PS eFUSE is successful.
<code>0xFFFFZZZZ</code>	Represents PS eFUSE is not initiated and PL eFUSE is process returned with error.
<code>0xYYYYFFFF</code>	Represents PL eFUSE is not initiated and PS eFUSE is process returned with error.

For Zynq UltraScale+ MPSoC, the status in the `xilsky_bbramps_zynqmp_example.c`, `xilsky_puf_registration.c` and `xilsky_efuseps_zynqmp_example.c` files is conveyed as 32 bit error code. Where Zero represents that no error has occurred and if the value is other than Zero, a 32 bit error code is returned.

Procedures

This chapter provides detailed descriptions of the various procedures.

Zynq eFUSE Writing Procedure Running from DDR as an Application

This sequence is same as the existing flow described below.

1. Provide the required inputs in `xilskey_input.h`, then compile the SDK project.
2. Take the latest FSBL (ELF), stitch the `<output>.elf` generated to it (using the bootgen utility), and generate a bootable image.
3. Write the generated binary image into the flash device (for example: QSPI, NAND).
4. To burn the eFUSE key bits, execute the image.

Zynq eFUSE Driver Compilation Procedure for OCM

The procedure is as follows:

1. Open the linker script (`lscript.ld`) in the SDK project.
2. Map all the chapters to point to `ps7_ram_0_S_AXI_BASEADDR` instead of `ps7_ddr_0_S_AXI_BASEADDR`. For example, Click the Memory Region tab for the `.text` chapter and select `ps7_ram_0_S_AXI_BASEADDR` from the drop-down list.
3. Copy the `ps7_init.c` and `ps7_init.h` files from the `hw_platform` folder into the example folder.
4. In `xilskey_efuse_example.c`, un-comment the code that calls the `ps7_init()` routine.
5. Compile the project.
The `<Project name>.elf` file is generated and is executed out of OCM.

When executed, this example displays the success/failure of the eFUSE application in a display message via UART (if UART is present and initialized) or the reboot status register.

UltraScale eFUSE Access Procedure

The procedure is as follows:

1. After providing the required inputs in `xilskey_input.h`, compile the project.
2. Generate a memory mapped interface file using TCL command `write_mem_info`

```
$Outfilename
```

3. Update memory has to be done using the tcl command `updatemem`.

```
updatemem -meminfo $file.mmi -data $Outfilename.elf -bit $design.bit  
-proc design_1_i/microblaze_0 -out $Final.bit
```

4. Program the board using `$Final.bit` bitstream.
5. Output can be seen in UART terminal.

UltraScale BBRAM Access Procedure

The procedure is as follows:

1. After providing the required inputs in the `xilskey_bbram_ultrascale_input.h` file, compile the project.
2. Generate a memory mapped interface file using TCL command

```
write_mem_info $Outfilename
```

3. Update memory has to be done using the tcl command `updatemem`:

```
updatemem -meminfo $file.mmi -data $Outfilename.elf -bit $design.bit  
-proc design_1_i/microblaze_0 -out $Final.bit
```

4. Program the board using `$Final.bit` bitstream.
5. Output can be seen in UART terminal.

Additional Resources and Legal Notices

Xilinx Resources

For support resources such as Answers, Documentation, Downloads, and Forums, see [Xilinx Support](#).

Solution Centers

See the [Xilinx Solution Centers](#) for support on devices, software tools, and intellectual property at all stages of the design cycle. Topics include design assistance, advisories, and troubleshooting tips.

Please Read: Important Legal Notices

The information disclosed to you hereunder (the "Materials") is provided solely for the selection and use of Xilinx products. To the maximum extent permitted by applicable law: (1) Materials are made available "AS IS" and with all faults, Xilinx hereby DISCLAIMS ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, OR FITNESS FOR ANY PARTICULAR PURPOSE; and (2) Xilinx shall not be liable (whether in contract or tort, including negligence, or under any other theory of liability) for any loss or damage of any kind or nature related to, arising under, or in connection with, the Materials (including your use of the Materials), including for any direct, indirect, special, incidental, or consequential loss or damage (including loss of data, profits, goodwill, or any type of loss or damage suffered as a result of any action brought by a third party) even if such damage or loss was reasonably foreseeable or Xilinx had been advised of the possibility of the same. Xilinx assumes no obligation to correct any errors contained in the Materials or to notify you of updates to the Materials or to product specifications. You may not reproduce, modify, distribute, or publicly display the Materials without prior written consent. Certain products are subject to the terms and conditions of Xilinx's limited warranty, please refer to Xilinx's Terms of Sale which can be viewed at <http://www.xilinx.com/legal.htm#tos>; IP cores may be subject to warranty and support terms contained in a license issued to you by Xilinx. Xilinx products are not designed or intended to be fail-safe or for use in any application requiring fail-safe performance; you assume sole risk and liability for use of Xilinx products in such critical applications, please refer to Xilinx's Terms of Sale which can be viewed at <http://www.xilinx.com/legal.htm#tos>.



Automotive Applications Disclaimer

AUTOMOTIVE PRODUCTS (IDENTIFIED AS "XA" IN THE PART NUMBER) ARE NOT WARRANTED FOR USE IN THE DEPLOYMENT OF AIRBAGS OR FOR USE IN APPLICATIONS THAT AFFECT CONTROL OF A VEHICLE ("SAFETY APPLICATION") UNLESS THERE IS A SAFETY CONCEPT OR REDUNDANCY FEATURE CONSISTENT WITH THE ISO 26262 AUTOMOTIVE SAFETY STANDARD ("SAFETY DESIGN"). CUSTOMER SHALL, PRIOR TO USING OR DISTRIBUTING ANY SYSTEMS THAT INCORPORATE PRODUCTS, THOROUGHLY TEST SUCH SYSTEMS FOR SAFETY PURPOSES. USE OF PRODUCTS IN A SAFETY APPLICATION WITHOUT A SAFETY DESIGN IS FULLY AT THE RISK OF CUSTOMER, SUBJECT ONLY TO APPLICABLE LAWS AND REGULATIONS GOVERNING LIMITATIONS ON PRODUCT LIABILITY.

© Copyright 2018 Xilinx, Inc. Xilinx, the Xilinx logo, Artix, ISE, Kintex, Spartan, Virtex, Vivado, Zynq, and other designated brands included herein are trademarks of Xilinx in the United States and other countries. All other trademarks are the property of their respective owners.