

confidential for Frilling

confidential for Frame

CV181x/CV180x eFuse 使用指南

Version: 0.4

Release date: 2023-02-06

© 2023 北京晶视智能科技有限公司 本文件所含信息归<u>北京晶视智能科技有限公司</u>所有。 未经授权,严禁全部或部分复制或披露该等信息。

al for White



修订记录

	: 2)			
. 761	iti		· Jents	· Jentra
	Revision	Date	Author	Description
	0.1	2022-06-01		Initial
	0.2	2022-09-28	Leon.liao	Rename chip
	0.3	2023-02-01	Leon.liao	更新安全启动 efuse 烧录流程
	0.4	2023-02-06	Leon.liao	CV181x/CV180x 文档融合

al for 深圳睡士

Fidential for This thing to Confidential for This thing to

Confidential for TRHIME!

for 深圳雁十



法律声明

本数据手册包含北京晶视智能科技有限公司(下称"晶视智能")的保密信息。未经授权,禁止使用或披露本数据手册中包含的信息。如您未经授权地需合物式如义(2011) 能遭受任何损失或损害,您应对因之产生的损失/损害承担责任。

for 深圳種子

本文件内信息如有更改,恕不另行通知。晶视智能不对使用或依赖本文件所含信息承担任何责 任。

本数据手册和本文件所含的所有信息均按"原样"提供,无任何明示、暗示、法定或其他形式 的保证。晶视智能特别声明未做任何适销性、非侵权性和特定用途适用性的默示保证,亦对本 数据手册所使用、包含或提供的任何第三方的软件不提供任何保证; 用户同意仅向该第三方寻 求与此相关的任何保证索赔。此外,晶视智能亦不对任何其根据用户规格或符合特定标准或公 开讨论而制作的可交付成果承担责任。

Confidential for Fithing t

for 深圳便士



目录

	80	27			601		601	
0,1	97						antial	
	丁记录	•••••		· <u>.</u>	•••••		2	
法律	車声明	•••••	Con	•••••		C_{Or}	3	
目表	₹	•••••		•••••	•••••	•••••	4	
1	eFus	e 使用指	南	•••••	•••••	•••••	5	
	1.1	eFuse ⁷	概述				5	
	1.2	安全启	动 eFuse 设定流和	呈			6	
		1.2.1	查看密钥内容	•••••			6	
		1.2.2	写入密钥	•••••			6	
		1.2.3	使能安全启动	•••••		•••••	7	
	1.3	eFuse (u-boot 命令参考.				7	
	1.4	eFuse /	API 参考				8	
	1.5	数据类	型				14	
				idential			ential for	

FOT 深圳雁

Confidential for Athlet



eFuse 使用指南 1

1.1 eFuse 概述

Confidential for Fither 芯片内部集成 eFuse 空间,可供安全启动和和 448 bits 的用户自定义区域。 具体 eFuse 分区请参考表格 1 和表格 2。

Confident'i

<u> </u>	lame	Size	Comment	
l	JSER	40 Bytes	用户自定义区域	
	DEVICE_ID	8 Bytes	装置序号	
F	HASH0_PUBLIC	32 Bytes	验签所需 SHA256 摘要	
L	OADER_EK	16 Bytes	加密密钥	
	DEVICE_EK	16 Bytes	用户自定义区域,可被锁定	1種子
S	SECUREBOOT	4 Bytes	使能安全启动	· · · · · · · · · · · · · · · · · · ·
Confidential fo	IZ V	表格 1 eFuse	用户可写入区域	ial for ikilling t
	Name	Comme		
	LOCK HASHO PU	BLIC 锁定 HA	ASHO_PUBLIC,让此区域无法读写	

for 深圳随

表格 1 eFuse 用户可写入区域

	dentila
Name	Comment
LOCK_HASH0_PUBLIC	锁定 HASHO_PUBLIC,让此区域无法读写
LOCK_LOADER_EK	锁定 LOADER_EK,让此区域无法读写
LOCK_DEVICE_EK	锁定 DEVICE_EK,让此区域无法读写
SECUREBOOT	使能安全启动

表格 2 eFuse 安全设定字段

for 深圳種



1.2 安全启动 eFuse 设定流程

注意事项

晶视智能提拱 u-boot 命令和 Linux 库两种方式存取 eFuse,下列流程以 u-boot 命令作为范

1.2.1 查看密钥内容

在 PC 上查看密钥内容:

* 查看加解密秘钥

host\$ xxd -p -c 256 loader ek.key

668f8b6655a89f7cb8ee5cbd6f2c914e

- * 获取验签所需 sha256 值
- * 执行签署脚本 fipsign.py 时, 脚本会打印所需 sha256 值,如下:

host\$./fipsign.py

Host\$

onfidential for Tathlhe Host\$ INFO:root:KPUB HASH:978bc2031b9377dadb4c7c34467ee985806a63a3ac8ee293a3f0eddcd2b7 89d8

Host\$

1.2.2 写入密钥

1. 写入 loader_ek.key 进 eFuse 的 "加密密钥" 区域,数据为 16 个数组,以 16 进 位表示成 32 个数字。如果未使用加密功能可跳过这步骤。

u-boot# efusew LOADER_EK 668f8b6655a89f7cb8ee5cbd6f2c914e

2. 写入验签所需 sha256 值进 eFuse 的 "验签所需 SHA256 摘要" 区域,数据为 32 个数组,以16进位表示成64个数字

Confider

u-boot# efusew HASH0_PUBLIC 978bc2031b9377dadb4c7c34467ee985806a63a3ac8ee293a3f0eddcd2b789d8

3. 锁定密钥区域,防止读写

u-bootx# efusew LOCK_LOADER_EK 01

u-boot# efusew LOCK_HASH0_PUBLIC 01

^{*} KPUB_HASH: 后面的字符串就是所需 sha256 值

Confidential for TEHIMET



1.2.3 使能安全启动

* enable 安全启动 签署/验签 功能

u-boot# efusew SECUREBOOT 01

* enable 安全启动 签署/验签 和 加密/解密 功能

u-boot# efusew SECUREBOOT 02

*注意:加密/解密功能开启后无法关闭,需要和签署和加密后的 FIP.bin 配合使用,只签署的 FIP.bin 无法烧录和启动

注意事项

Confidential for Fride 安全启动使能后无法再变更,烧录前请注意已签署/加密过 FIP 镜像

1.3 eFuse u-boot 命令参考

u-boot 提供以下命令存取 eFuse

- efuser: 倾印 eFuse 区域。
- efusew:写入eFuse区域。

efuser

【描述】

倾印 eFuse 区域。

【语法】

efuser EFUSE_AREA

【参数】

E_AREA			
参数名称	602		E O. K.M.
EFUSE_AREA	eFuse 区域名称,	参考表格1和表格2。	+121 1
	onfident 7	Cou	Eiden

confidential for



打印用户自定义区域数据

Confidential for TRHME cv181x/cv180x# efuser USER 00000020: 00 00 00 00 00 00 00 00 cv181x/cv180x#

efusew

【描述】

将数据写入 eFuse 区域。

【语法】

efuser EFUSE AREA DATA

【参数】

			-
	参数名称	描述	
	EFUSE_AREA	eFuse 区域名称,参考表格 1 和表格 2。	111/1111
	DATA	用于写入 eFuse 的数据,以 16 进位表示	深圳
		1 500	- for
【举例】			
将数据 03020	01 写入用户自定义	区域	ijde,
cv181x/cv180	0x# efusew USER 03	0201	
Write eFuse I	JSFR(0) with:		

【举例】 将**·"

Write eFuse USER(0) with:

00000000: 03 02 01

cv181x/cv180x# efuser USER

00000020: 00 00 00 00 00 00 00 00

cv181x/cv180x#

1.4 eFuse API 参考

eFuse API 位于 CIPHER 模块,提供以下 API

- CVI_EFUSE_Read: 读取 eFuse 区域大小。

 CVI_EFUSE_Read: 读取 eFuse 区域大小。
- <u>CVI_EFUSE_Read</u>: 读取 eFuse 区域。
- CVI_EFUSE_Write: 写入 eFuse 区域。
- CVI_EFUSE_EnableSecureBoot: 使能安全启动。

confidential for TRIMMET



- CVI_EFUSE IsSecureBootEnabled: 查询安全启动状态。
- CVI_EFUSE_EnableFastBoot: 使能快速启动。
- CVI_EFUSE_IsFastBootEnabled: 查询快速启动状态。
- CVI_EFUSE_Lock: 锁定 eFuse 区域。
- CVI EFUSE IsLocked: 查询 eFuse 区域是否被锁定。

CVI_EFUSE_GetSize

【描述】

查询 eFuse 区域大小。

【语法】

CVI_S32 CVI_EFUSE_GetSize(CVI_EFUSE_AREA_E area, CVI_U32 *size);

【参数】

参数名称		描述		弃	俞入/辅	出	
area		指定 eFuse 🛭	区域		输入	•	
size	THE Y	eFuse 区域大小 (单	位:字节)	面十	输出		
可值》			for Athle	W)			
7	返回值	1	描	述		· dentia	
	>= 0	fidence	成	功			
	< 0	$Co_{M_{\mathcal{L}}}$	参考:	错误码	Co_{λ}		

【返回值】 Confidential

返回值	12	描述
>= 0	fiden	成功
< 0	Cour	参考错误码

【需求】

头文件: cvi_type.h cvi_unf_cipher.h

库文件: libcipher.a

【注意】

无。

【举例】

参考 sample_efuse.c。

CVI_EFUSE_Read

【描述】

读取 eFuse 区域。

【语法】

CVI_S32 CVI_EFUSE_Read(CVI_EFUSE_AREA_E area, CVI_U8 *buf, CVI_U32 buf_size);

【参数】 Confident

参数名称	描述	输入/输出
area	指定 eFuse 区域	输入



v	ns are subject te	oriange without notice		
			#	山桶
	参数名称	描述	输入/输出	(宋)
\	buf	用于存放 eFuse 数据	输出	7 60z
	buf_size	数据的长度(单位:字节)	输入	

Confidential 【返回值】

返回值	描述
>= 0	成功
< 0	参考错误码

【需求】

头文件: cvi_type.h cvi_unf_cipher.h

库文件: libcipher.a

【注意】

无。

【举例】

参考 sample_efuse.c。

CVI_EFUSE_Write

fidential for *###### Fidential for Filmer 写入 eFuse 区域。 【语法】 CVI_S32 CVI_EFUSE_Write(CVI_EFUSE_AREA_E area, const CVI_U8 *buf, CVI_U32 buf_size);

【参数】

参数名称	描述	输入/输出
area	指定 eFuse 区域	输入
buf	用于写入 eFuse 的数据	输入
buf_size	数据的长度(单位:字节)	输入

【返回值】

返回值	描述	
>= 0	成功	
< 0	参考错误码	
vpe.h cvi_unf_ciph oher.a		
	10	

【需求】

头文件: cvi_type.h cvi_unf_cipher.h 库文件: libcipher.a

Confidential for This William



【注意】

无。

802

参考 sample_efuse.c。

CVI_EFUSE_EnableSecureBoot

【描述】

使能安全启动。

【语法】

CVI_S32 CVI_EFUSE_EnableSecureBoot(void);

【参数】

无

【返回值】

返回值	描述	
>= 0	安全启动已使能	
< 0	参考错误码	
With the same of t	深圳榧	深圳種
ype.h cvi_unf_cipher.h oher.a		nfidential for William

【需求】

库文件: libcipher.a 【注意】 ~ 头文件: cvi_type.h cvi_unf_cipher.h

【举例】

参考 sample_efuse.c。

CVI_EFUSE_IsSecureBootEnabled

【描述】

判断安全启动是否已使能。

【语法】

CVI_S32 CVI_EFUSE_IsSecureBootEnabled(void);

【参数】

无

元 【返回值】			
	返回值	描述	
	> 0	安全启动已使能	
	0	安全启动尚未使能	£01
· Jentia	<0 dentire	参考错误码	. dential
	Confile	Cox	til
	1	1	

Confidential for This William



【需求】

confidential for *** ###### 头文件: cvi_type.h cvi_unf_cipher.h

库文件: libcipher.a

【注意】

无。

【举例】

参考 sample_efuse.c。

CVI_EFUSE_EnableFastBoot

【描述】

使能快速启动。

【语法】

CVI_S32 CVI_EFUSE_EnableFastBoot(void);

【参数】

无。

【返回值】

参数值	描述	
0	快速启动已使能	
< 0	参考错误码	
pe.h cvi_unf_ciphe	dentia: Confi	

confidential for Thy 头文件: cvi_type.h cvi_unf_cipher.h

库文件: libsys.a

【注意】

无。

【举例】

参考 sample_fastboot.c。

注意事项

快束启动使能后无法再变更

CVI_EFUSE_IsFastBootEnabled

【描述】

判断快速启动是否已使能。

【语法】

for深圳艇十 CVI_S32 CVI_EFUSE_IsFastBootEnabled(void); _vi_S32 【参数】 于 Confiden

Confidential for White



【返回值】	川便十		深圳種土	深圳恒生
	返回值	1	描述	For
	0	intia	快速启动已使能	intial
	< 0	nfide	快速启动尚未使能	rider.
	•	Cas	C)

【需求】

头文件: cvi_type.h cvi_unf_cipher.h

库文件: libsys.a

【注意】

无。

【举例】

参考 sample_efuse.c。

CVI_EFUSE_Lock

【描述】

锁定 eFuse 区域。

【语法】

for深圳砸十 CVI_S32 CVI_EFUSE_Lock(CVI_EFUSE_LOCK_E lock);;

【参数】

EFUSE_Lock 杜】 eFuse 区域。 去】 532 CVI_EFUSE 故】	_Lock(CVI_EFUSE_LOCK_E lock);;		L FOR FRIME
参数名称	描述	输入/输出	
area	指定要锁定的 eFuse 区域	输入	

【返回值】

返回值	描述	
>= 0	指定的 eFuse 分区已锁定	
< 0	参考错误码	

【需求】

confidential for Frimmet 头文件: cvi_type.h cvi_unf_cipher.h

库文件: libcipher.a

【注意】

Confider充。 【举例】

Confidential for The Hilling to



CVI_EFUSE_IsLocked 【描述】

こ。 IsLocked 【描述】 查询 eFuse 区域是否被锁定。 【语法】 CVI_S32 CVI_EFIIC

【参数】

参数名称	描述	输入/输出
area	指定要锁定的 eFuse 区域	输入

【返回值】

返回值	描述	
> 0	指定的 eFuse 分区已锁定	
0	指定的 eFuse 分区尚未锁定	11
< 0	参考错误码	深圳伽
/pe.h cvi_unf_c oher.a	ipher.h	

【需求】

头文件: cvi_type.h cvi_unf_cipher.h

库文件: libcipher.a

【注意】

无。

【举例】

参考 sample_efuse.c。

1.5 数据类型

相关数据类型、数据结构定义如下:

- CVI_EFUSE_AREA_E: 定义 eFuse 区域
- CVI_EFUSE_LOCK_E: 定义各 eFuse 区域对应的锁定 Confidential for TRIMET

CVI EFUSE AREA E

【说明】

定义 eFuse 区域。

【定义】

typedef enum {

Confidential for While t



CVI_EFUSE_AREA_LAST } CVI_EFUSE_AREA_E;

【成员】

成员名称	描述	
CVI_EFUSE_AREA_USER	用户自定义区域	
CVI_EFUSE_AREA_DEVICE_ID	装置序号	
CVI_EFUSE_AREA_HASH0_PUBLIC	U-BOOT 验签所需 SHA256 摘要	
CVI_EFUSE_AREA_LOADER_EK	U-BOOT 加密密钥	山植土
CVI_EFUSE_AREA_DEVICE_EK	用户自定义区域,可被锁定	THE STATE OF THE S
CVI_EFUSE_AREA_LAST	无效的区域	9 ₇
【注意事项】	Contide	-

Confident 【注意事项】

无。

【相关数据类型及接口】

CVI_EFUSE_GetSize, CVI_EFUSE_Read, CVI_EFUSE_Write

CVI_EFUSE_LOCK_E

【说明】

定义 eFuse 区域。

【定义】

typedef enum {

Confidential for TRIMET CVI_EFUSE_LOCK_HASH0_PUBLIC,

CVI_EFUSE_LOCK_LOADER_EK,

CVI_EFUSE_LOCK_DEVICE_EK,

CVI_EFUSE_LOCK_LAST

ZVI_EFUSE_LO

CVI_EFUSE_LOCK_E;



【成员】

 【成员】	深圳腫	深圳腫土
成员名称	描述	02
CVI_EFUSE_LOCK_HASH0_PUBLIC	锁定 U-BOOT 验签所需 SHA256 摘要	
CVI_EFUSE_LOCK_LOADER_EK	锁定 U-BOOT 加密密钥	
CVI_EFUSE_LOCK_DEVICE_EK	锁定用户自定义区域,可被锁定	
CVI_EFUSE_LOCK_LAST	无效的锁定	

【注意事项】

无。

【相关数据类型及接口】

CVI_EFUSE_Lock, CVI_EFUSE_IsLocked

Confidential for While t