代码加密以及操作方法介绍

Rev 1.2

DISCLAIMER

All information and data contained in this document are without any commitment, are not to be considered as an offer for conclusion of a contract, nor shall they be construed as to create any liability. Any new issue of this document invalidates previous issues. Product availability and delivery are exclusively subject to our respective order confirmation form; the same applies to orders based on delivered development samples delivered. By this publication, Shanghai Mountain View Silicon Co., Ltd.("MVSILICON") does not assume responsibility for patent infringements or other rights of third parties that may result from its use.

Shanghai Mountain View Silicon Co., Ltd. Assumes no responsibility for any errors contained herein.

Revision History

Date	Revision	Author	Description
2013-12-11	v1.0	ZHAO Ying (Alfred)	Initial
2013-12-12	v1.1	ZHAO Ying (Alfred)	Name modification to "USB encryption dongle" in the figure of encryption process
2014-2-27	v1.2	Jack Zhao	面向国内用户的中文版本 增加密钥烧录的操作说明

Contents

1. 简介

山景 AP 系列音频处理器具有一种可靠的代码加密保护机制，能够有效保护存储在外部 FLASH 中的代码，从而防止用户的知识产权受到侵害。

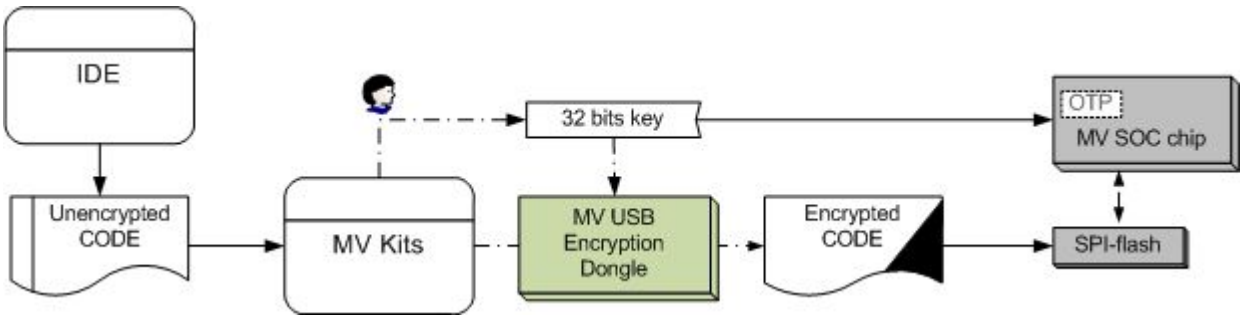
2. 代码加密机制

通过一个用户给定的 32 位密钥，将源代码加密成密文后存储在外部 FLASH 中，并且将该 32 位密钥烧入 AP 芯片内部的密钥存储器中，只有当密钥与外部 FLASH 的密文完全匹配时，芯片才能正常运行。AP 芯片内部的密钥存储器采用一次性熔断机制，因此不能读取。简而言之，没有正确的密钥，外部 FLASH 中的密文代码就算被克隆也是不能使用的。

2.1 加密过程

图 1 描绘了一个完整的加密操作过程。详细的过程描述如下：

图 1 加密过程



山景的代码加密工具链包括：一个 PC 端软件，一个 USB 加密狗，一个密钥烧录工具。

1. 生成未加密的明文代码
   基于山景提供的 SDK，用户使用 ARM CM3 的开发工具（如 MDK），编译生成未加密的代码。代码文件请以二进制（bin）形式存在。

2. 生成密文代码

用户需要用到山景工具链中的 PC 软件和 USB 加密狗。打开 PC 软件，在 CODE 操作区，载入未加密的二进制代码，将 USB 加密狗插入电脑 USB 端口，提示窗口会提示发现加密狗。输入 32 位密钥到密钥输入框。启动加密，经过一段时间运算后，加密狗将密文传回 PC 软件。请务必记住该 32 位密钥。

3. 密钥的烧录

请确保 PC 软件的密钥输入框中，是第 2 步中用于生成密文代码的密钥。连接好密钥烧录器后，点击 PC 软件的“Download KEY”按钮，打开密钥烧录器电源，电脑提示下载 OK。然后，可以使用该烧录器批量烧录 AP 芯片了。

4. 密文代码的烧录

密文代码和明文代码的烧录方式是一样的。要将第 2 步产生的密文代码烧录到 FLASH 中，请参考 FLASH 代码的烧录指导手册。

2.2 密文的解密运行

当 AP 系列芯片上电运行时，首先会将存储在密钥存储器内的 32 位密钥载入到芯片内部的硬件解密模块，当芯片开始从外部 FLASH 取值时，指令首先经过硬件解密模块解密，从而保证 CPU 能够正确的运行。因此，用户无需关心，也不能干预这个解密的过程。

2.3 不加密的数据区

用户通常需要在外部 FLASH 中存放一些字符点阵、开机音乐等数据。这些数据一般也无需加密，存储在不加密的数据区，山景称之为 CONSTANT 区。为此，山景 SDK 提供了一套读取不加密 FLASH 数据区的接口。

Contact Information

Shanghai Mountain View Silicon Co Ltd

Shanghai Headquarter:
Room 602,Building Y2,No.112 Liangxiu Road,Pudong,
Shanghai, P.R. China
Zip code: 201203
Tel: 86-21-68549851/68549853/68549857/61630160
Fax: 86-21-61630162

Shenzhen Sales & Technical Support Office:
Suite 6A Olympic Plaza, Shangbao Road, Futian District,
Shenzhen, Guangdong, P.R. China
Zip code: 518034
Tel: 86-755-83522955
Fax: 86-755-83522957

Email: support@mvsilicon.com
Website: http://www.mvsilicon.com