AN-1394
应用笔记

One Technology Way • P.O. Box 9106 • Norwood, MA 02062-9106, U.S.A. • Tel: 781.329.4700 • Fax: 781.461.3113 • www.analog.com/cn

用于ADF7023和ADF7023-J的AES加密与解密

作者：Stephen Hinchy 和 Kalim Khan

简介

本应用笔记说明ADF7023和ADF7023-J收发器可用的高级加密标准（AES）固件模块（在下文中，提到ADF7023的内容也适用于ADF7023-J）。可下载的AES固件模块支持密钥大小为128位、192位和256位的128位块加密和解密。它支持两种模式：电码本（ECB）模式和密码块链接（CBC）模式1。

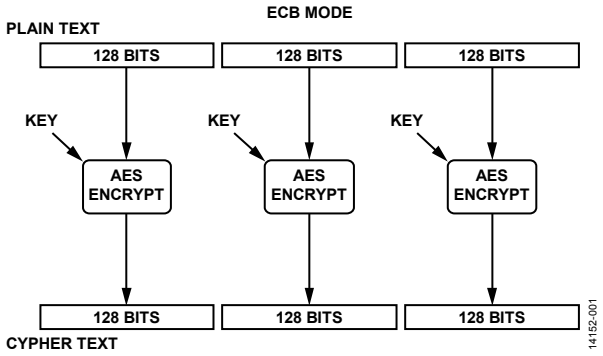

图1. ECB模式

ECB模式利用一个密钥逐块地加密和解密128位数据，如图1所示。CBC模式1则是先做一次加法运算（通过模2算法，用户提供的128位初始化向量）再加密，所得的密文用作下一个块的初始化向量，依此类推，如图2所示。

解密过程正好相反。固件利用片内硬件加速模块来增大吞吐量，并将AES处理的延迟时间降至最短。

该固件模块名为rom_ram_7023_2_2_RS_AES.dat，包含里德-所罗门（RS）前向纠错和AES加密，可从www.analog.com/firmwaremodules-adf7023下载。

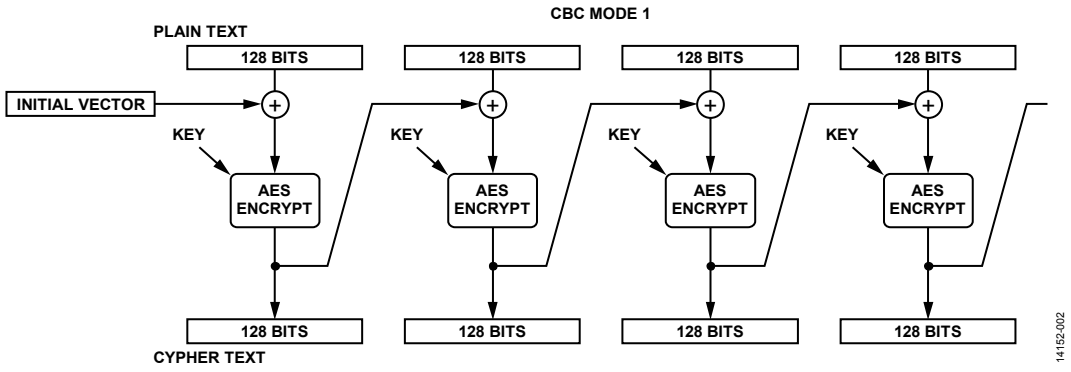

图2. CBC模式1

目录

修订历史

2016年2月—修订版0：初始版

命令和数据包随机存取存储器寄存器位置

表1. 需在AES加密或解密之前进行初始化的寄存器位置

寄存器地址[1]	寄存器名称	描述
0x001	VAR_NUM_BLOCKS	要加密或解密的16字节块数
0x010	VAR_C_PTR	要加密/解密的数据指针
0x011	VAR_W_PTR	32字节AES工作空间指针
0x012	VAR_WINV_PTR	逆密钥指针
0x013	VAR_WFOR_PTR	密钥指针
0x014	VAR_KEYSIZE	设置为0x0C（128位密钥）、0x14（192位密钥）或0x1C（256位密钥）
0x016	VAR_AES_MODE	设置为0x00（ECB模式）或0x01（CBC模式1）
0x017	VAR_ECV_PTR	128位初始化向量指针，用于CBC模式1加密
0x018	VAR_DCV_PTR	128位初始化向量指针，用于CBC模式1解密
0x019	VAR_CIPHERBUF_PTR	128位存储位置指针，利用CBC模式1解密时需要

[1] 这些寄存器定义针对该固件模块，不适用于ADF7023的正常操作。

AES配置变量、密钥和数据存储在数据包随机存取存储器(RAM)中。

表2中列出了执行AES加密、生成逆密钥或执行AES解密所需的命令。有关AES加密和解密步骤的更多信息，参见“AES步骤”部分。

由于使用指针、不同密钥大小和两种不同模式，ADF7023上的AES实现是高度可配置的。图3显示了一个配置示例。

表2. AES命令

命令	代码	描述
CMD_AES_ENCRYPT	0xD0	用于加密数据块的命令
CMD_AES_DECRYPT_INIT	0xD1	用于生成逆密钥的命令
CMD_AES_DECRYPT	0xD2	用于解密数据块的命令

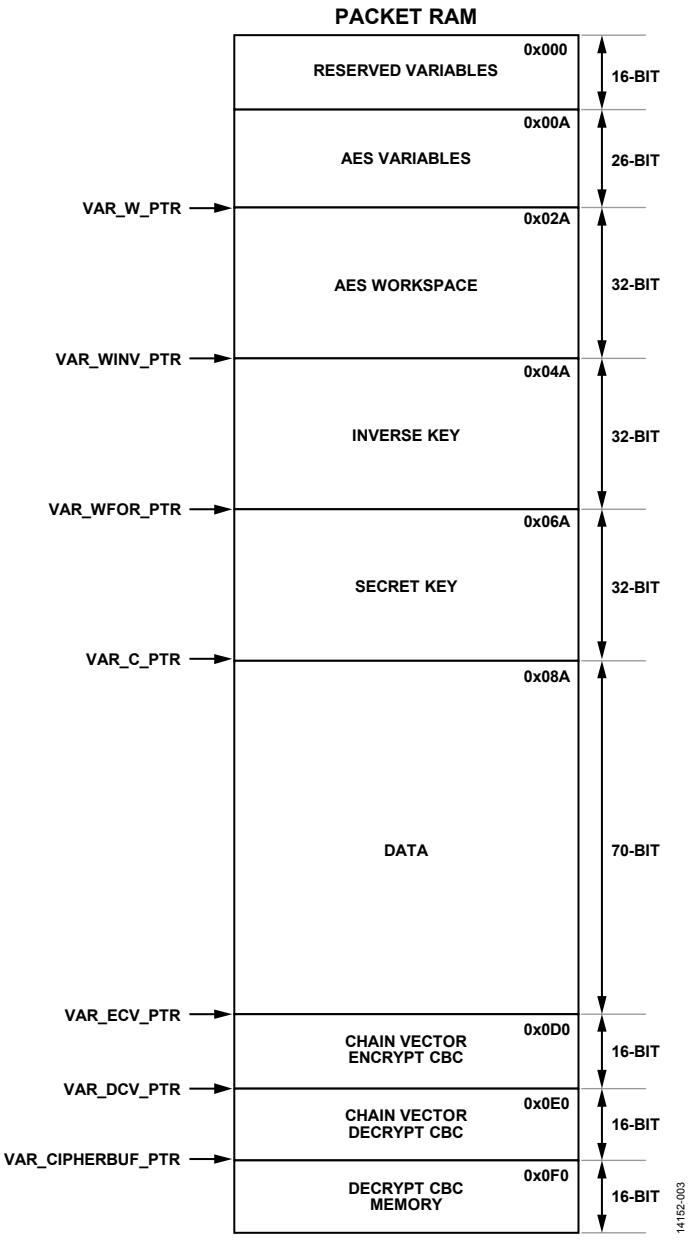

图3. AES操作的数据包RAM存储器分配示例

AES步骤

向ADF7023写入AES固件模块

使用AES固件模块之前，用户必须将其写入ADF7023的程序RAM中。下列步骤详细解释了如何向程序RAM写入AES固件模块：

1. 确保ADF7023处于PHY_OFF状态。
2. 发出CMD_RAM_LOAD_INIT命令（地址0xBF）。
3. 使用串行外设接口（SPI）存储器块写入命令（0x1E00[固件模块]）向程序RAM写入模块；有关块写入的更多信息，请参见ADF7023数据手册。
4. 发出CMD_RAM_LOAD_DONE命令（地址0xC7）。

固件模块现已存储到程序RAM中。

AES加密步骤

下列步骤详细说明了如何执行AES加密：

1. 将AES工作空间的起始地址写入VAR_W_PTR。
2. 写入VAR_KEYSIZE以设置密钥大小。
3. 写入VAR_AES_MODE以选择ECB模式或CBC模式1。
4. 若使用CBC模式1（若使用ECB模式则跳过此步），
   a. 将加密初始化向量的起始地址写入VAR_ECV_PTR。
   b. 将初始化向量写入VAR_ECV_PTR指定的位置。
5. 将密钥的地址写入VAR_WFOR_PTR。
6. 将密钥写入VAR_WFOR_PTR指定的位置。
7. 将要加密的16字节块数写入VAR_NUM_BLOCKS。
8. 将要加密的数据地址写入VAR_C_PTR。
9. 将要加密的数据写入VAR_C_PTR指定的位置。
10. 发出CMD_AES_ENCRYPT (0xD0)。用加密后的数据覆盖要加密的数据。
11. 等待命令完成。

AES加密示例

在下面的AES加密示例中，将SPI命令写入ADF7023：

1. 写入0x18112A。VAR_W_PTR设置为0x2A。算法的32字节工作空间从地址0x02A开始。
2. 写入0x18140C。通过VAR_KEYSIZE选择128位的密钥。
3. 写入0x181600。通过VAR_AES_MODE选择ECB模式。
4. 不使用CBC模式1，因此跳过第4步。
5. 写入0x18136A。VAR_WFOR_PTR设置为0x6A。密钥从地址0x06A开始。
6. 将密钥写入从地址0x06A开始的数据包RAM。
7. 写入0x180101。VAR_NUM_BLOCKS设置为0x01。加密一个16字节块。
8. 写入0x18108A。VAR_C_PTR设置为0x8A。要加密的数据从地址0x08A开始。
9. 将要加密的数据写入从地址0x08A开始的数据包RAM。
10. 写入0xD0。发出CMD_AES_ENCRYPT。
11. 等待命令完成。

AES解密步骤

下列步骤详细说明了如何执行AES解密：

1. 将AES工作空间的起始地址写入VAR_W_PTR。
2. 写入VAR_KEYSIZE以设置密钥大小。
3. 写入VAR_AES_MODE以选择ECB模式或CBC模式1。
4. 将密钥的地址写入VAR_WFOR_PTR。
5. 将密钥写入VAR_WFOR_PTR指定的位置。
6. 将逆密钥的地址写入VAR_WINV_PTR。
7. 若使用CBC模式1（若使用ECB模式则跳过此步），
   a. 将解密初始化向量的地址写入VAR_DCV_PTR。
   b. 将初始化向量写入VAR_DCV_PTR指定的位置。
   c. 将解密需要的保留存储地址写入VAR_CIPHERBUF_PTR。
8. 发出CMD_AES_DECRYPT_INIT (0xD1)。此命令生成并保存逆密钥。
9. 等待命令完成。
10. 将要解密的16字节块数写入VAR_NUM_BLOCKS。
11. 将要解密的数据地址写入VAR_C_PTR。
12. 将要解密的数据写入VAR_C_PTR指定的位置。
13. 发出CMD_AES_DECRYPT (0xD2)。用解密后的数据覆盖要解密的数据。
14. 等待命令完成。

AES解密示例

在下面的AES解密示例中，将SPI命令写入ADF7023：

1. 写入0x18112A。VAR_W_PTR设置为0x2A。算法的32字节工作空间从地址0x02A开始。
2. 写入0x18140C。通过VAR_KEYSIZE选择128位的密钥。
3. 写入0x181600。通过VAR_AES_MODE选择ECB模式。
4. 写入0x18136A。VAR_WFOR_PTR设置为0x6A。密钥从地址0x06A开始。
5. 将密钥写入从地址0x06A开始的数据包RAM。
6. 写入0x18124A。VAR_WINV_PTR设置为0x4A。逆密钥从地址0x04A开始。
7. 不使用CBC模式1，因此跳过第7步。

8. 写入0xD1。发出CMD_AES_DECRYPT_INIT。此命令生成并保存逆密钥，从地址0x04A开始。
9. 等待命令完成。
10. 写入0x180101。VAR_NUM_BLOCKS设置为0x01。解密一个16字节块。
11. 写入0x18108A。VAR_C_PTR设置为0x8A。要解密的数据从地址0x08A开始。
12. 将要解密的数据写入从地址0x08A开始的数据包RAM。
13. 写入0xD2。发出CMD_AES_DECRYPT。
14. 等待命令完成。

确定AES命令完成的时间

使用CMD_FINISHED中断来确定CMD_AES_ENCRYPT、CMD_AES_DECRYPT_INIT 和 CMD_AES_DECRYPT 命令何时完成。要使能该中断，请置位INTERRUPT_MASK_1寄存器（地址0x101）的位0 (CMD_FINISHED)。置位该屏蔽位后，ADF7023的中断引脚（IRQ_GP3）将在完成任何命令后置位。向INTERRUPT_SOURCE_1（地址0x337）的位0写入逻辑1可清除中断。有关中断产生的更多信息参见ADF7023数据手册。

AES加密和解密时间

典型AES执行时间如表3所示。

表3. AES初始化、加密和解密时间

数据长度（字节）	密钥大小（位）	初始化解密（ms）	加密（ms）	解密（ms）
16	128	1.08	1.07	1.22
	192	1.27	1.27	1.47
	256	1.47	1.46	1.69
32	128	1.08	2.13	2.42
	192	1.27	2.51	2.88
	256	1.46	2.87	3.37
48	128	1.08	3.19	3.61
	192	1.27	3.76	4.63
	256	1.46	4.3	5.05
64	128	1.08	4.24	4.82
	192	1.27	5.02	5.82
	256	1.46	5.76	6.72