GW2A(R)系列 FPGA 产品 AES 密钥编程指南

高云半导体 GW2A(R)系列 FPGA 产品支持数据流密文传输。

本文档主要介绍如何使用 Gowin Programmer 工具向 FPGA 产品中编程 AES（Advanced Encryption Standard）密钥、如何从 FPGA 中读取密钥、如何保证密钥安全以及整个 AES 密钥编程流程。

定义

- AES 密钥：也称 AES 私钥，AES 加密算法中用到的私钥部分，由算法外指定，本文简称 key；
- AES 密钥长度：128 位；
- Key：AES 密钥的简称，GW2A(R)系列 FPGA 产品中提供一个 128 位长度的地址用于存储 Key；
- LockMFG：为保证 AES 密钥的安全，该指令用于限制 key 的读写权限，本文将该过程简称 lock，当处于锁定状态后，任何对 key 的操作都将失效。

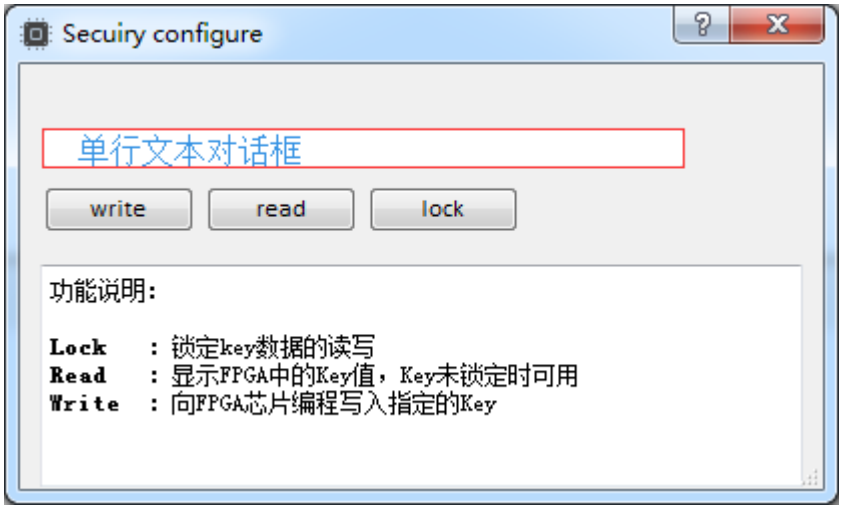
Gowin AES 加密特性

TBD

AES 密钥编程操作

Gowin Programmer 工具中提供了 AES 密钥编程工具，在 Gowin 云源软件中单击菜单“Tools”中“Security”选项即可开启该工具，如图 1 所示。

图 1 AES 编程对话框



该程序包含三个功能，分别是：

- Write：编程 Key；
- Read：读取 Key；
- Lock：锁定 Key 的读写权限。

编程 Key（Write）

1. 将自定义的 Key(AES 密钥)填入“单行文本对话框”中；
2. 单击“write” 按钮；
3. 工具运行结束，返回验证结果。

读取 Key（Read）

单击“read”按钮可对写入的 AES 密钥进行再次验证，读取出来的 AES 密钥会显示在“单行文本对话框”中。

锁定 Key（Lock）

单击“lock”按钮，锁定 Key 数据的读写，AES 密钥将不能再被读取和写入。

AES 密钥编程流程

图 2~图 6 给出了如何编程 AES 密钥或 MFG Data 流程，图示流程均基于 JTAG 协议。

图 2 Prepare

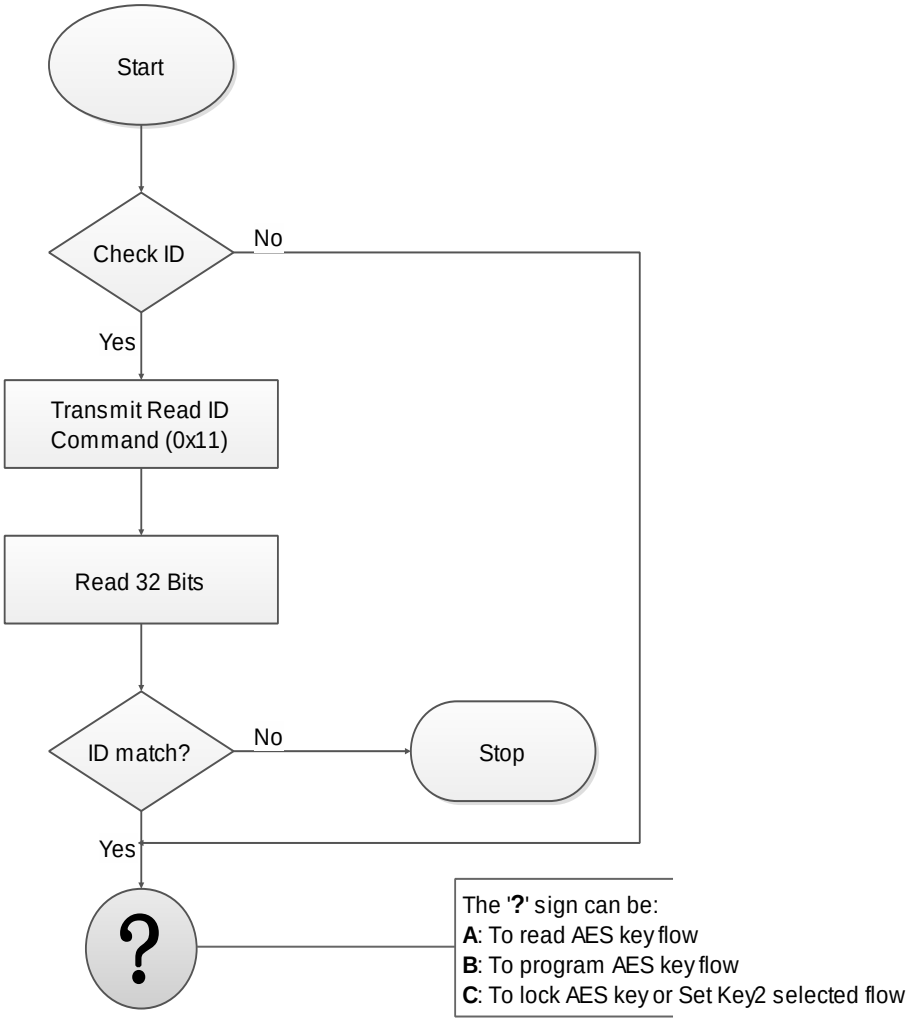


图 3 Read AES Key Flow

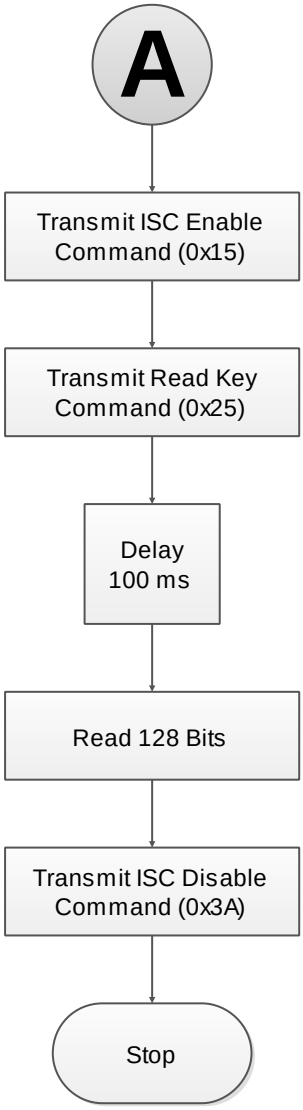


图 4 Program AES Key Flow

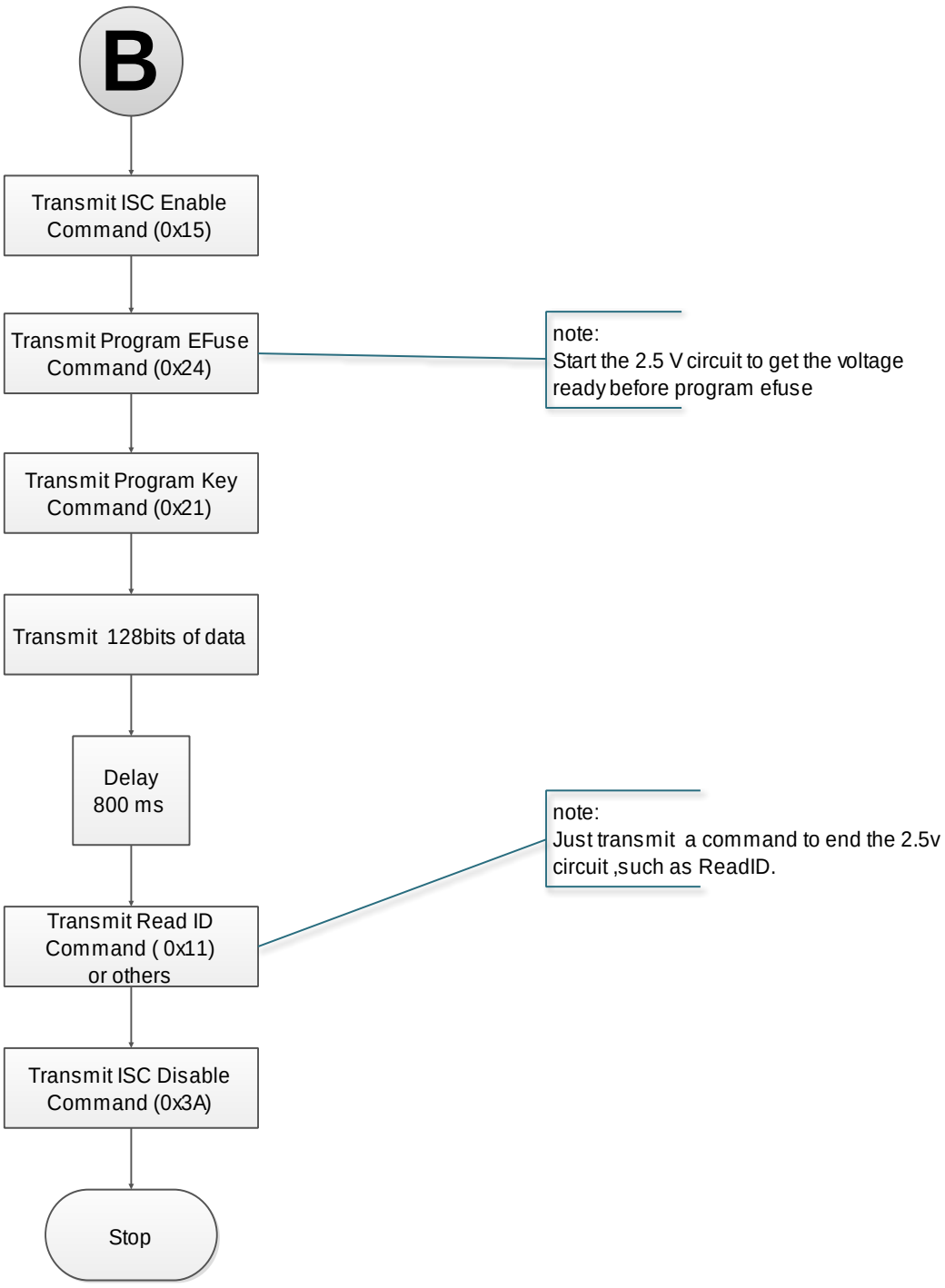


图 5 Lock AES Key Flow

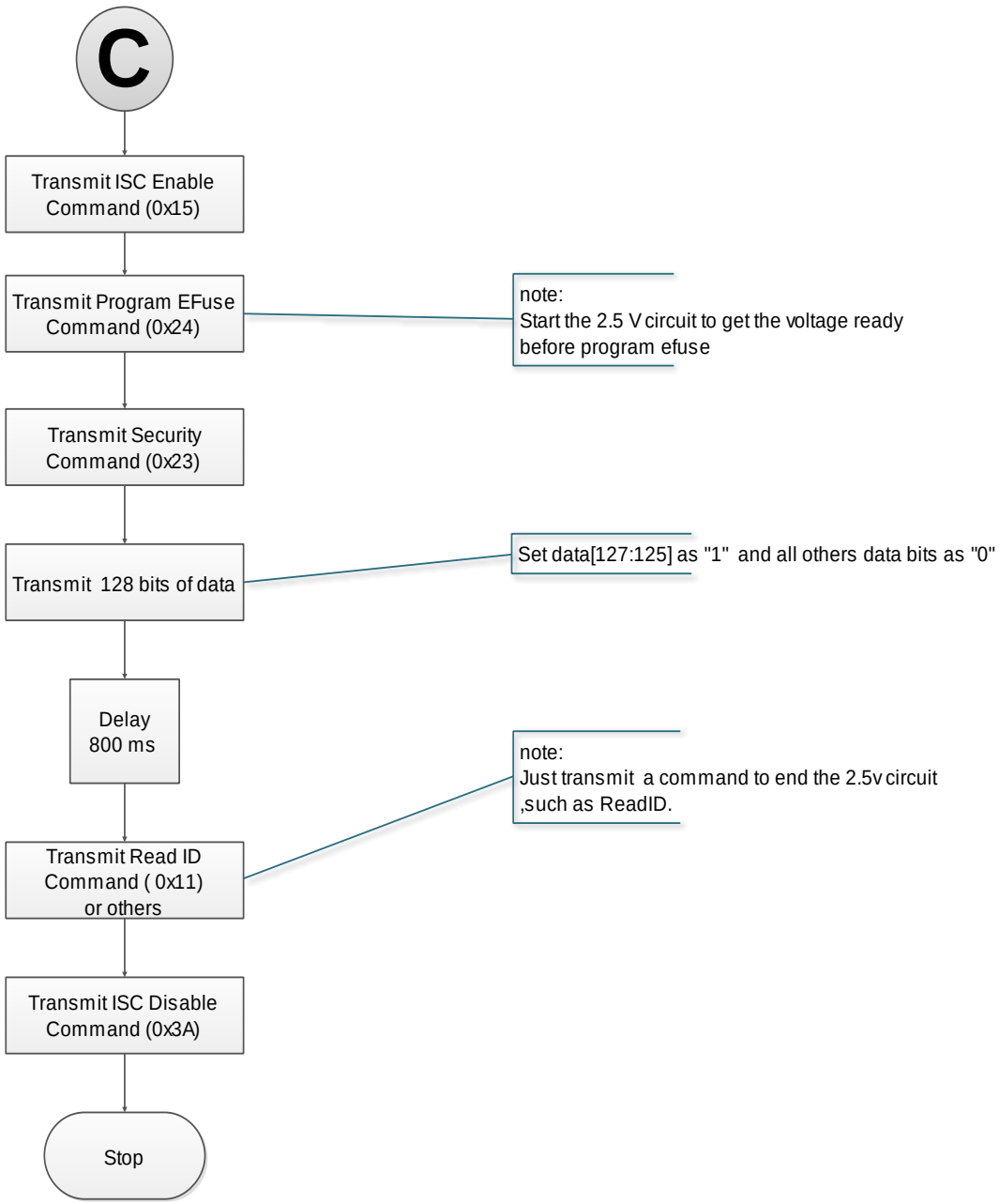
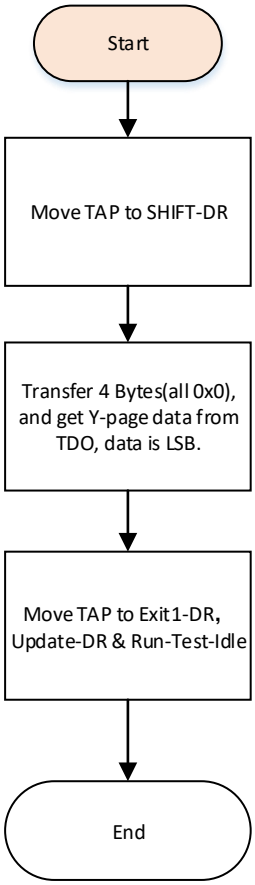


图 6 读取一个 Y-page 的过程



技术支持与反馈

高云半导体提供全方位技术支持，在使用过程中如有任何疑问或建议，可直接与公司联系：

网址：www.gowinsemi.com.cn

E-mail：support@gowinsemi.com

Tel：00 86 0755 82620391

版本信息

日期	版本	说明
2018/08/09	1.0	初始版本。

免责声明

本文档并未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除高云半导体在其产品的销售条款和条件中声明的责任之外，高云半导体概不承担任何法律或非法律责任。高云半导体对高云半导体产品的销售和／或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性、适销性或对任何专利权、版权或其它知识产权的侵权责任等，均不作担保。高云半导体对文档中包含的文字、图片及其它内容的准确性和完整性不承担任何法律或非法律责任，高云半导体保留修改文档中任何内容的权利，恕不另行通知。高云半导体不承诺对这些文档进行适时的更新。