基于 CHIP ID 的 FPGA 加密算法设计与实现

陈小宇，叶佳栋
（华中师范大学 物理科学与技术学院，湖北 武汉 430079）

摘 要： 针对 FPGA 芯片上电配置数据容易被窃取的问题，提出了一种基于 CHIP ID 的加密算法。CHIP ID 是 Altera 公司 Cyclone V 系列 FPGA，出厂就带有的唯一 ID，调用 IP 核就可以读出每个芯片的 ID。此 ID 可以根据开发者的需求加入个性化加密算法并与指定 FPGA 结合起来，生成配置比特流文件。主程序运行自定义加密算法计算出一个加密值，将加密值与预存的匹配值进行对比，判断程序是否正常运行。结果表明使用 CHIP ID 加密的方法具有稳定高效、简单可靠和资源占用少等优点。

关键词： CHIP ID；FPGA 实现；加密
中图分类号： TN409　　**文献标识码：** A　　**DOI：**10.16157/j.issn.0258-7998.200419

中文引用格式： 陈小宇，叶佳栋. 基于 CHIP ID 的 FPGA 加密算法设计与实现[J].电子技术应用，2020，46(11)：100-103.
英文引用格式： Chen Xiaoyu，Ye Jiadong. Design and implementation of FPGA encryption algorithm based on CHIP ID[J]. Application of Electronic Technique，2020，46(11)：100-103.

Design and implementation of FPGA encryption algorithm based on CHIP ID

Chen Xiaoyu，Ye Jiadong
（College of Physical Science and Technology，Central China Normal University，Wuhan 430079，China）

Abstract： Aiming at the problem that FPGA chip power-on configuration data is easily stolen，an encryption algorithm based on CHIP ID is proposed. CHIP ID is the unique ID that comes with Altera′s Cyclone V series FPGAs.Each CHIP ID can be read by calling the IP core，this ID can be added to the personalized encryption algorithm according to the needs of developers and combined with the specified FPGA to generate configuration bitstream files. The main program runs a custom encryption algorithm to calculate an encrypted value，compares the encrypted value with the pre-stored matching value，and judges whether the program is running normally.The results show that the method using CHIP ID hardware encryption has the advantages of high-stability，high-efficiency，high-reliability，and less resource occupation.

Key words： CHIP ID；FPGA implementation；encryption

0 引言

近年来，现场可编程门阵列(Field Programmable Gate Array，FPGA)凭借着它卓越的性能、灵活方便的可升级特性得到了广泛的应用。大部分 FPGA 器件采用了查找表(Look Up Table，LUT)结构，其物理结构是静态随机存取存储器(Static Random-Access Memory，SRAM)[1]，它要求每次上电重新对 FPGA 进行配置，二进制配置文件从外部存储器加载到内部 SRAM 中运行，这就使得监视配置的位数据流成为可能[2]。因此必须加上保密技术保护开发者的知识产权。

主流的 FPGA 加密策略有外置安全辅助芯片法、内置密钥法和 DEVICE ID 与比特流封装法三种[3]。外置安全辅助芯片法通过将 FPGA 与外置安全辅助芯片相结合，同时在各自内部产生随机密钥并进行安全哈希算法计算，在 FPGA 内部进行匹配校验完成加密[4]。安全芯片一般是 CPU 或者专用芯片等，此类方法对读写时序和寄存器配置要求严格，对开发者水平要求较高[5]。内置密钥法原理是利用 FPGA 内置密钥与高级加密标准(Advanced Encryption Standard，AES)的方式对配置数据比特流加密，一般是高端 FPGA 芯片采用的方法。这种加密方法加密效果好但对成本敏感的应用场合来说不太合适[6]。DEVICE ID 与比特流封装法是将每个 FPGA 带有的唯一 ID 与设计关联起来，设计者可以加入自定义算法，实现加密过程。此加密方法对 Xilinx 和 Altera 公司的多数 FPGA 都适用，区别在于它们对于 DEVICE ID 的命名不同，Xilinx 和 Altera 的命名分别为 DEVICE DNA 和 CHIP ID。DEVICE ID 与比特流封装法具有使用移植简单、占用资源少和适用性广的特点。

本文针对当前电子设备的发展现状，以 Altera 公司的 FPGA 为例，设计了一种基于 CHIP ID 的加密方式。为优化系统结构，节省逻辑资源，本文采用了硬件电路和逻辑控制的设计方式，同时结合自定义加密方法，实现

了对 FPGA 加密的过程。

1 系统总体设计方案

Cyclone V 系列所有 FPGA 出厂都会带有的一组唯一的 64 bit 二进制数值，它就是 CHIP ID。本文根据这个 ID，将加密过程分为密码存储和密码校验两个工程，实现了对 FPGA 的加密。图 1 所示为加密原理图。

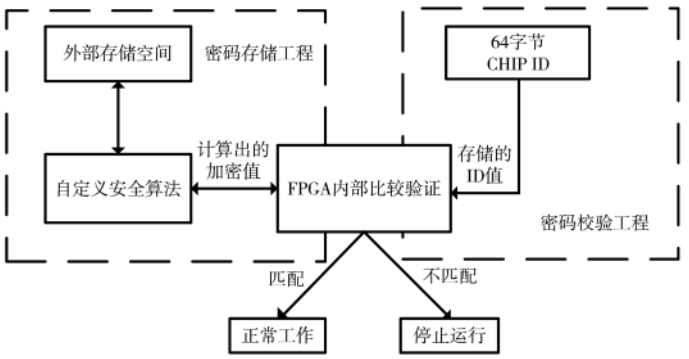

图 1 加密原理图

密码存储工程的主要功能是 FPGA 读出 CHIP ID 值并加密存入外部存储器中。此工程只运行一次，将密码存入存储器中它的工作就已完成。

密码校验工程的主要功能是 FPGA 读出外部存储器加密后的数据并按相同加密逻辑进行反算，同时读出 CHIP ID 值，将两个数据进行对比，返回一个校验值。为1表示校验通过，程序正常运行；为 0 表示校验失败，程序停止运行。

2 系统硬件设计

为实现加密流程，本文硬件系统设计由 FPGA 配置电路和外部存储器构成。FPGA 配置电路以 FPGA 为核心，配合一片串行 Flash 工作，保证 FPGA 上电后完成配置正常运行[7]。外部存储器使用了带电可擦可编程只读存储器(Electrically Erasable Programmable read only memory，EEPROM)，它的主要作用是存储加密后的 CHIP ID。系统电路结构如图 2 所示。

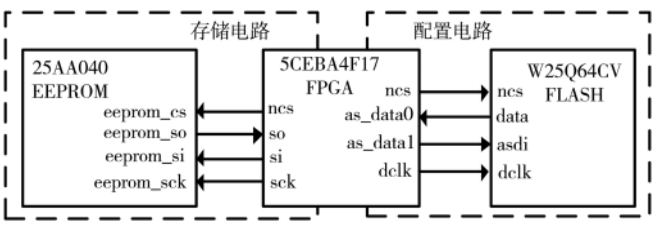

图 2 系统电路结构图

2.1 FPGA 配置电路设计

配置电路完成主要的功能是系统上电后将配置数据流加载到 FPGA 上。本文采用 Altera 公司推荐的片外串行 Flash 下载方式，在每片 FPGA 周围放置一片或几片串行 Flash，系统上电时 FPGA 自动读取 Flash 中的配置文件[8]。采用的 Flash 芯片型号为 W25Q64CV，它的存储空间为 64 Mb，并且最高支持同时扩展四片 Flash，完成 256 Mb 超大容量扩展，基本覆盖各种工程的需求。它的主要引脚说明如表 1 所示。

表 1 引脚说明

引脚名	方向	描述
ncs	I	芯片选择引脚
data	O	串行配置数据输出
asdi	I	串行配置数据输入
dclk	I	配置时钟

2.2 外部存储电路设计

外部存储电路完成的主要功能是将 CHIP ID 值读出并存储到 EEPROM 中，在 FPGA 上电配置完成后再读出存入 EEPROM 的值。本文选用的 EEPROM 芯片型号为 25AA040A，使用 SPI 通信协议，它的容量是 4 KB，在一些对数据量要求不大的工程中使用较为广泛。

3 FPGA 实现

3.1 密码存储工程的 FPGA 实现

密码存储工程实现主要分为两步，分别是读出 CHIP ID 值和将读出值加密后写入 EEPROM 中。密码存储流程图如图3 所示。

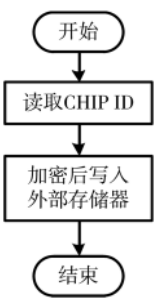

图 3 密码存储流程图

3.1.1 读 CHIP ID

读取 CHIP ID 需要调用 IP 核，它一共有四个端口，分别是输入时钟和复位信号，输出 64 位 chip_id 值和数据有效 data_valid 信号。想要正确地读出 ID 值，时钟要求最大不超过 100 MHz，复位为高有效且至少要保持 10 个时钟周期，当复位结束后，data_valid 引脚会拉高，表示数据有效，此时 ID 值会锁存在 chip_id 引脚，用户即可成功采集 chip id 值。读取 CHIP ID 时序图如图 4 所示。

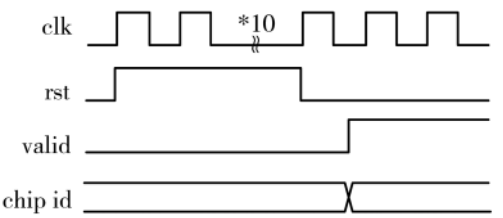

图 4 CHIP ID 读取时序图

3.1.2 加密逻辑

FPGA 的 CHIP ID 每个开发者都可以读出，如果不将它进行加密处理，那么窃取者将很容易从二进制配置流文件中找到此值，只需更改相应位置的比特流，将其发送到另一块相同型号的 FPGA 中就能达到窃取的目的。

因此，读出 CHIP ID 后，需要将读出的数据加密后再写入 EEPROM 中。经过加密处理后的值与原始值的形态大小都已改变，想要在庞大的二进制文件中找到它相当困难，这样就起到了对 FPGA 加密的作用。

加密原则是将读出来的初始值打乱顺序、改变数据长度和，起到隐藏原始值的作用。本文采用的是首尾交换、中间取反结合异或运算的加密逻辑，具体加密过程举例如图 5 所示。对比发现，12 位二进制初始值转换为十六进制值为 0x9DA，加密后的值为 0xA6F，起到了加密的作用。

图 5 加密过程示例

3.1.3 写 EEPROM

本文使用的 EEPROM 的型号为 25AA040，主要用于存储一些寄存器配置或小批量数据，具有使用灵活、可靠性高的特点。它最高支持 16 个字节的页读和页写模式，只需给一次地址即可连续读写 128 bit 数据。本文设计中要存储的加密值为 64 bit，需要用到它的页写模式，写时序如图 6 所示。

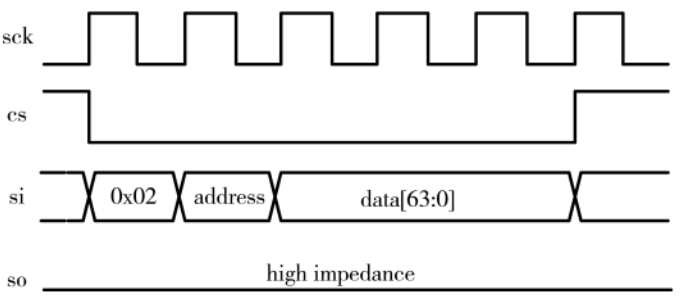

图 6 EEPROM 写时序图

该芯片支持 SPI 时序，cs 为片选控制信号，so 为串行输出信号，si 为串行输入信号，sck 为串行时钟。具体流程是，cs 拉低后发送写使能（0x02）和写地址，紧接着发送要写入指定地址的数据，写完成后拉高 CS 并保持一段时间写完成[9]。

3.2 密码校验工程的 FPGA 实现

密码校验工程就是最终 FPGA 要执行的程序，它包含了读出 EEPROM 值并解算出初始值和密码校验两步。密码校验工程流程图如图 7 所示。

3.2.1 读 EEPROM

读 EEPROM 和写时序差不多，不同的是读的时候需要同时使用 si 和 so 引脚，而在写 EEPROM 的时候不需要管 so 引脚。具体流程是cs 拉低后发送读使能(0x03)，紧接着发送读地址，这时在 so 引脚就可以读出数据了。读时序如图 8 所示。

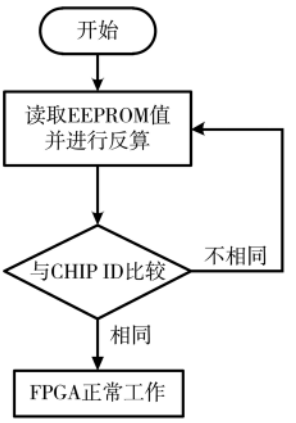

图 7 密码校验工程流程图

3.2.2 解密与密码校验

读出数据后，首先需要将数据解密。解密方法用了最简单的反向运算法，只需将密码值按照设定的加密逻辑反向运算一次即可得到初始值。校验过程需要调用读 CHIP ID 的 IP 核，读出 CHIP ID 值并与解密值对比，判断程序是否正常运行。

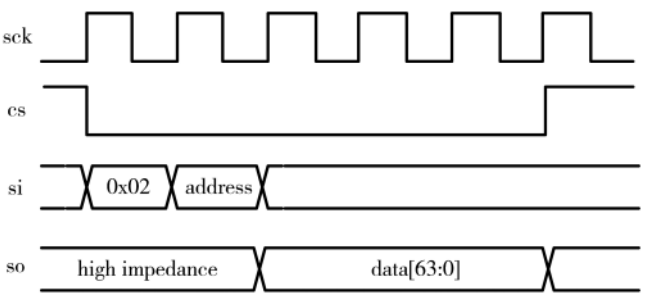

图 8 EEPROM 读时序图

3.3 系统仿真与验证

整个工程在 Quartus II 18.1 开发环境中设计开发，结合自带的仿真软件 Signal Tap 进行仿真。测试时钟选择 10 MHz，经过测试系统功能实现正常。图 9 和图 10分别为工程加入加密算法前后逻辑资源使用对比图。图11为结果验证图。

Family	Cyclone V
Device	5CEBA4F17I7
Timing Models	Final
Logic utilization (in ALMs)	2,635 / 18,480 (14 %)
Total registers	2974
Total pins	54 / 128 (42 %)

图 9 加入加密算法前资源使用图

Family	Cyclone V
Device	5CEBA4F17I7
Timing Models	Final
Logic utilization (in ALMs)	3,720 / 18,480 (20 %)
Total registers	3470
Total pins	54 / 128 (42 %)

图 10 加入加密算法后资源使用图

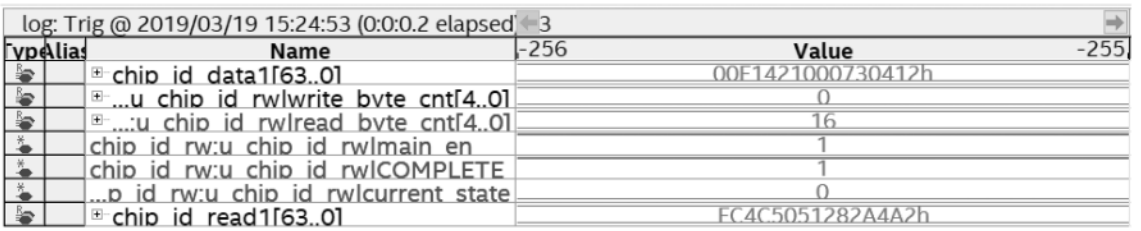

图 11 结果验证图

比较可以看出，加密逻辑规模较小，加入后没有对FPGA性能造成太大影响。

上电后，系统首先读出写入EEPROM中的匹配值，即图11中chip_id_read1；然后调用IP核读出芯片CHIP ID值，即图中chip_id_data1；chip_id_data1经过加密算法运算后得到加密值，将此值与匹配值进行对比得到一个校验值，即main_en，为1表示校验通过，FPGA正常工作。从图中可以看出，上电后加密逻辑工作正常，起到保护FPGA的作用。

4 结论

本文介绍了一种使用CHIP ID进行FPGA加密的方法，并重点介绍了实现过程。该方法能很好地适用于满足硬件条件的工程，具有较强的实用性。使用双工程的设计使得整套工程移植起来十分方便，同时加入加密功能后对逻辑资源占用较少，不影响FPGA的正常工作。还可以根据项目需要加入不同安全性能的加密算法，使整个项目安全性更高。

参考文献

[1] 马群刚，杨银堂，李跃进，等.基于LUT的SRAM-FPGA结构研究[J].电子器件，2003(1)：10-14.

[2] 杨海钢，孙嘉斌，王慰.FPGA器件设计技术发展综述[J].电子与信息学报，2010，32(3)：714-727.

[3] 蒲恺，徐文杰，李大鹏，等.基于FPGA的知识产权保护方法研究及实现[J].电子技术，2013，40(4)：12-15.

[4] 王沁，孙富明，李磊，等.FPGA设计安全性综述[J].小型微型计算机系统，2010，31(7)：1333-1337.

[5] 刘宇，徐东明，王艳，等.基于1-Wire总线的DS28E01加密芯片原理研究及其在FPGA加密系统中的应用[J].电子产品世界，2014，21(Z1)：47-49.

[6] 杨春林，张春雷，高山，等.基于DS28E01的FPGA加密认证系统的设计[J].微计算机信息，2009，25(23)：129-130，215.

[7] 赵勇，孟李林，李小龙.Cyclone Ⅳ系列FPGA的配置方式及其工程应用[J].微型机与应用，2013，32(19)：25-28.

[8] 李鹏，兰巨龙.用CPLD和Flash实现FPGA配置[J].电子技术应用，2006(6)：101-103.

[9] 关珊珊，周洁敏.基于Xilinx FPGA的SPI Flash控制器设计与验证[J].电子器件，2012，35(2)：216-220.

(收稿日期：2020-05-26)

作者简介：

陈小宇(1972-)，男，博士，副教授，主要研究方向：嵌入式系统与应用、信号与信息处理、高速信号采集。

叶佳栋(1996-)，男，硕士研究生，主要研究方向：嵌入式系统与应用。

(上接第99页)

[9] 傅军栋，陈俐，康水华，等.基于蜻蜓算法和支持向量机的变压器故障诊断[J].华东交通大学学报，2016，33(4)：103-112.

[10] 吴伟民，吴汪洋，林志毅，等.基于增强个体信息交流的蜻蜓算法[J].计算机工程与应用，2017(4)：10-14.

[11] 龙文，梁昔明，龙祖强，等.基于改进蚁群算法优化参数的LSSVM短期负荷预测[J].中南大学学报(自然科学版)，2011，42(11)：3408-3414.

[12] 杨冰芳，薛琢成.考虑噪声数据的FCM-LSSVM负荷预测模型[J].电力科学与工程，2017(11)：12-17.

[13] 公政，姜文，王来河，等.基于BA-LSSVM的短期电力负荷预测研究[J].电子质量，2017(3)：1-4.

[14] 龙金莲，卢家暄，张玉分，等.基于GMDH-PSO-LSSVM中长期电力负荷预测[J].贵州大学学报(自然版)，2017，34(6)：49-53.

[15] 郝晓弘，刘鹏娟，汪宁渤.混沌优化PSO-LSSVM算法的短期负荷预测[J].兰州理工大学学报，2019(1)：85-90.

[16] 孔祥玉，李闯，郑锋，等.基于经验模态分解与特征相关分析的短期负荷预测方法[J].电力系统自动化，2019，43(5)：75-85.

[17] 司刚全，李水旺，石建全，等.采用改进果蝇优化算法的最小二乘支持向量机参数优化方法[J].西安交通大学学报，2017，51(6)：14-19.

(收稿日期：2020-01-13)

作者简介：

徐少波(1972-)，男，本科，工程师，主要研究方向：电子技术应用。

李鑫(1988-)，男，本科，工程师，主要研究方向：配网运行。

刘海涛(1984-)，男，本科，助理工程师，主要研究方向：配网检修。

版权声明