一种新的 SRAM 工艺 FPGA 的保护方法

董春国
(枣庄科技职业学院 电气工程系，山东 枣庄 277500)

摘 要：针对 SRAM 工艺 FPGA 应用中的安全问题，提出了一种采用双重认证(身份认证和产权认证)的保护方法。不仅能够使得非法者无法使用 FPGA，而且有效防止 IP 核被盗用。在 FPGA 外部添加安全芯片，负责完成身份认证，确认使用者的合法性；在 IP 核内添加保护模块，与安全芯片交互完成产权认证，确认 IP 核的合法性。详细介绍了双重认证方法的思想、原理和实现过程，并进行了安全性分析。

关键词：FPGA；IP 核；保护；双重认证
中图分类号：TP331 文献标识码：A 文章编号：1674-7720(2012)18-0020-03

A new protection method of SRAM-based FPGA

Dong Chunguo
(Department of Electrical Engineering, Zaozhuang Vocational College of Science & Technology, Zaozhuang 277500, China)

Abstract: For the security problem of SRAM-based FPGA, a new protection method is purposed in this paper, which uses double authentication—user authentication and property authentication. The method can prevent unauthorized user from using the system as well as the IP core from being stolen. Legality of user is assured by the extern security device, while legality of IP core is assured through the communication between protection module in IP core and the extern security device. The idea, principle and implementation are demonstrated, and a security analysis is applied on the method.

Key words: FPGA; IP core; protection; double authentication

在电子产品设计中，FPGA 由于灵活方便、性能突出等优点，得到了越来越广泛的应用。目前，市场占有率最高的两大公司 Xilinx 和 Altera 生产的 FPGA 大都是基于 SRAM 工艺的，而 SRAM 工艺 FPGA 由于自身的特点，存在诸多安全问题[1]。因此，实际应用中需要采取一定的保护手段，确保 SRAM 工艺 FPGA 的安全应用。

1 SRAM 工艺 FPGA 的安全问题

SRAM 工艺 FPGA 具有掉电易失性，在实际的应用中需要外部存储器来存储其配置信息。因此，SRAM 工艺的 FPGA 具有可反复使用、升级方便、配置电路简单等优点。然而，由于 FPGA 的配置电路及时序是公开的，在 FPGA 加载配置信息的过程中，不法者可以通过侦测 FPGA 配置管脚，截取配置信息来配置其他 FPGA。而配置信息是设计者 IP 核的具体表现形式，这样，IP 核被非法复制，使设计者的产权受到破坏。

针对该问题，参考文献[2]提出一种结合 EDA 软件和 FPGA 的方法，有效防止 IP 核被非法复制；参考文献[3]在 IP 核中添加保护模块，通过保护模块和外部验证设备通信认证来确认 IP 核的合法性。以上文献从不同方面对 IP 核的防复制进行了研究[4]，但都未对使用 FPGA 的用户进行身份认证。由于 FPGA 通常作为电子系统的核心或关键模块，为合法用户提供一定的服务，因此，实际应用中需对使用 FPGA 的用户进行身份认证。本文对此提出一种采用双重认证(身份认证、产权认证)的保护方法，以满足 SRAM 工艺 FPGA 防止非法用户使用及 IP 核防复制的双重需求。

2 双重认证方法的设计

2.1 双重认证方法的思想及模型

由于 FPGA 芯片供应商对配置数据流的定义是不公开的，所以无法通过配置数据流推测内部电路。因此需要在 IP 核中添加保护模块，使得配置成功后 FPGA 先不工作，只有在身份认证、产权认证成功后，FPGA 才正常工作。双重认证方法既认证使用者的合法性，又认证 IP 核的合法性，确保 SRAM 工艺 FPGA 的安全应用。

本设计需要在 IP 核中嵌入保护模块，同时在 FPGA 外添加安全芯片。系统上电后，从配置器件加载 IP 核到

FPGA，IP 核中的工作电路暂时不能工作，只有当产权认证成功，保护模块发出使能信号，IP 核中工作电路才开始工作。产权认证由 IP 核中保护模块和外部的安全管理芯片交互实现，而身份认证则由安全管理芯片完成。双重认证方法模型如图 1 所示，主要包括 FPGA、FPGA 配置器件、安全芯片等。

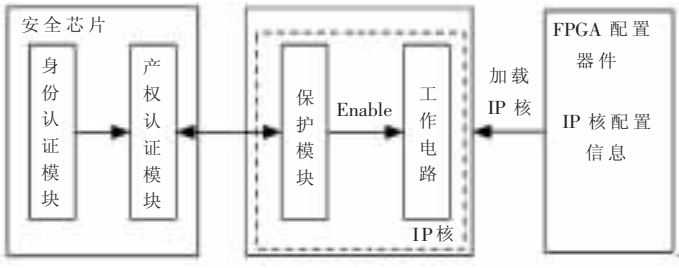

图 1 双重认证方法模型

本设计中，对 FPGA 及其配置器件无特殊要求，选用通用器件即可，这里选用的分别是 Altera 公司的 EP2C20F256C8 和 EPCS1。

安全芯片既要实现身份认证，又要通过与 IP 核中保护模块的交互实现产权认证，对安全性及其他性能都有较高的要求。本设计选用 Z32 芯片作为安全芯片。

2.2 双重认证方法的工作流程

本设计采用双重认证机制保护 FPGA 的安全应用，其工作流程如图 2 所示。系统上电后，从存储器件加载 IP 核到 FPGA 中，首先进行用户身份认证，身份认证成功后进行产权认证。只有当身份认证和产权认证全部成功后，FPGA 才开始正常工作。两次认证中任意一次失败，就会启动错误计数器，当计数达到设定的值后，系统就会销毁存储的秘密信息，使得系统失效。

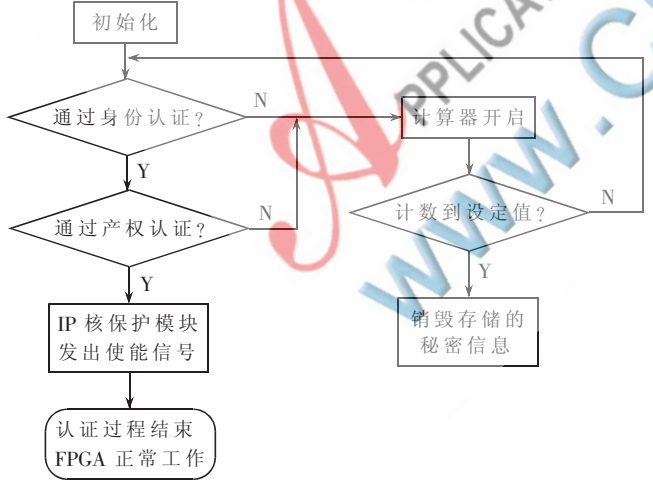

图 2 双重认证方法工作流程

从图 2 可以看出，产权认证受身份认证保护，即只有身份认证通过，才能进行产权认证。不法者即使获得 IP 核配置信息，由于不能通过身份认证，也无法使 FPGA 正常工作；合法使用者如果复制 IP 核的配置信息来配置其他 FPGA，由于不能通过产权认证，也无法使 FPGA 正常工作。因此，双重认证方法有效地满足了 SRAM 工艺 FPGA 的安全应用需求。

3 关键模块的设计及实现

首先对以下两个符号进行说明：

(1) K_p：口令密钥，在身份认证成功后由口令、口令哈希值等分量合成，主要用于对密文存在的认证密钥 K_a 解密。

(2) K_a：认证密钥，受口令密钥 K_p 保护，身份认证成功前以密文形式存在，是产权认证过程中 AES 算法的密钥。

3.1 身份认证模块

身份认证主要由 Z32 安全芯片来完成。本设计在 Z32 的固件程序中，实现 AES 算法和 SHA-256 算法。在芯片的 Flash 中开辟安全存储区，只有固件控制程序可以对该安全存储区操作，外部程序无访问权限。为了提高身份认证的安全性，本设计采用口令方式进行身份认证，安全存储区中不存储口令的明文，仅存储正确口令的哈希值及认证密钥 K_a 的密文。

身份认证原理如图 3 所示。本设计采用了密钥分级保护的思想，通过口令密钥 K_p 来保护认证密钥 K_a。只有用户口令正确，系统才能计算出口令密钥 K_p，然后调用 AES 算法将认证密钥 K_a 解密；若口令不正确，则即使将系统暴力拆解，直接读取芯片的存储区，也只能获得 K_a 的密文，而无法获得 K_a 的值。

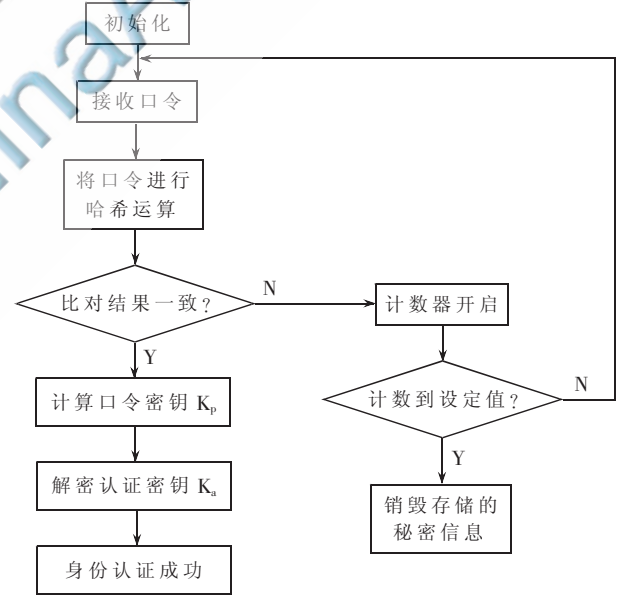

图 3 身份认证原理图

身份认证的具体过程为：

(1) 接收用户输入的口令。

(2) 将用户输入的口令用 SHA-256 算法处理，其结果与安全存储区中正确口令的哈希值 (256 bit) 进行比对。若比对结果一致，则跳过步骤(3)，否则执行步骤(3)。

(3) 重新执行步骤(1)，同时启动错误计数器，错误

值加 1。当计数到设定值，则销毁安全存储区中的数据，系统被锁死。

(4) 将口令与哈希值的低 128 bit 按位异或，得口令密钥 K_p。若口令值不足 128 bit，则将口令高位补为 0，补足 128 bit；若口令多于 128 bit，则仅取其低 128 bit。

(5) 调用 AES 算法，用步骤(4)得到的口令密钥 K_p 将密文存储的 K_a 解密，得认证密钥 K_a。解密后的 K_a 也存储在安全 Flash 区中。同时，Z32 芯片将生成的口令密钥 K_p 清零。

(6) 身份认证成功，向 IP 核保护模块发出产权认证开始信号，等待其响应。

若身份认证成功后，用户输入修改登录口令的命令，则首先用原口令密钥 K_p 将认证密钥 K_a 解密，然后计算出新口令的哈希值及新的口令密钥 K_p，调用 AES 算法将认证密钥 K_a 用新的口令密钥加密，最后将安全存储区中数据用新口令的哈希值和 K_a 新的密文替换。在这里需要注意的是认证密钥 K_a 的值并未变化，改变的仅为存储区中 K_a 的密文。

3.2 产权认证模块

产权认证由 Z32 芯片和 IP 核中的保护模块共同完成，产权认证原理如图 4 所示，虚线为控制信号，实线为数据流。IP 核保护模块由伪随机数发生器、AES 加/解密器、比对模块、比对结果处理模块、寄存器等组成。当用户通过身份认证后，Z32 芯片将安全存储区中加密存储的认证密钥 K_a 解密，然后通知 FPGA，FPGA 响应该信号，即产权认证开始。

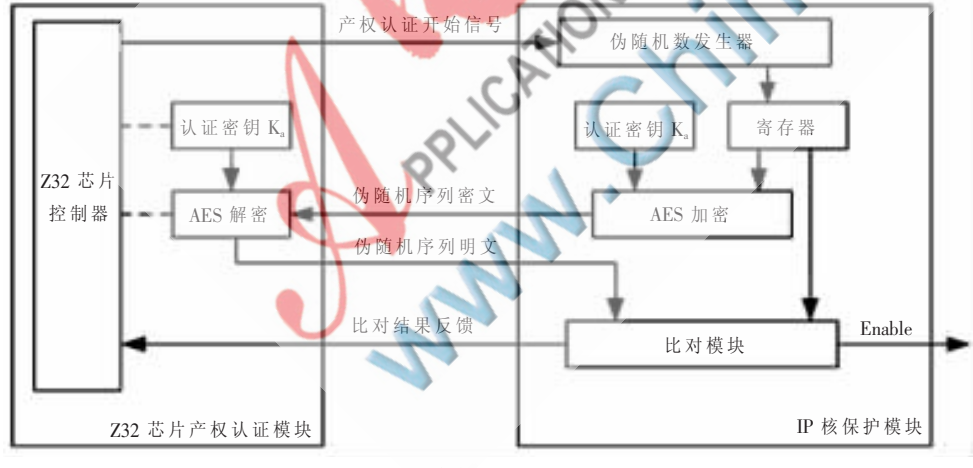

图 4 产权认证原理图

产权认证的具体过程为：

(1) Z32 芯片向 FPGA 发出产权认证开始信号。

(2) IP 核保护模块响应产权认证开始信号，伪随机数发生器产生一个伪随机序列。

(3) 伪随机序列分成两路：一路存储在保护模块的寄存器中；另一路用 AES 算法加密(其中加密密钥为 K_a)，然后把密文传给 Z32 芯片。

(4) Z32 芯片接收到密文后，利用身份认证过程中解密所得的认证密钥 K_a，将所接收到的密文解密，然后将结果回传给 FPGA 认证模块。

(5) IP 核保护模块接收到 Z32 传回的序列，将其与步骤(1)中产生的序列值比对。若比对结果一致，则发出使能信号，IP 核中工作电路开始工作；若不一致，则比对模块向 Z32 控制器传回比对错误信号，重新执行步骤(1)，同时 Z32 芯片启动错误计数器，错误值加 1，当计数到设定值，则销毁 Z32 安全存储区中的信息，系统被锁死。

4 安全性分析

本设计中，IP 核工作电路只有在产权认证成功后才能工作，由于产权认证采用了挑战应答方式，每次产生的随机序列不同，非法者使用重放攻击不能通过产权认证。由于对伪随机序列采用的是 AES 加密，在不知道密钥的情况下很难破解，安全可靠性高[5]。因此，产权认证的安全性取决于认证密钥 K_a 的安全性。

认证密钥 K_a 存在于 FPGA 的配置数据流和安全芯片中。因为 FPGA 芯片供应商对配置数据流的定义是不公开的，所以无法获得配置数据流中的认证密钥 K_a。而若想破解安全芯片而获得认证密钥 K_a 也是不现实的，因为 K_a 受口令密钥 K_p 保护，只有用户输入正确的口令，才能利用口令、口令哈希值计算出口令密钥 K_p，才能将 K_a 解密。非法用户没有正确的口令，不能计算出口令密钥 K_p，无法使 FPGA 正常工作，这样便达到了防止非法用户使用 FPGA 的目的；合法用户通过身份认证后能够将 K_a 解密，但只有固件程序能够对 K_a 操作，用户也无法获得 K_a 的具体值，即使拷贝 IP 核配置信息来配置其他 FPGA，由于不知道 K_a 的具体值，无法通过产权认证，复制的 IP 核也不能工作，实现了对设计者产权的保护。

本文设计的保护方法采用了身份认证、产权认证两重认证机制，体现了分级保护的思想。虽然消耗了一部分硬件资源，但有效地保证了 SRAM 工艺 FPGA 的安全应用，达到了非法用户不能使用 FPGA、合法用户不能侵犯设计者产权的目的。本设计安全性高、通用性强，具有广泛的应用前景。

参考文献

[1] GUAJARDO J,KUMAN S, SCHRIJEN S, et al. Physical unclonable functions and public-key crypto for FPGA IP protection[C]. Amsterdam: Field Programmable Logic and application, 2007: 189-195.

[2] 章礼宏，范全润. 基于 EDA 软件和 FPGA 的 IP 核保护

技术[J]. 电子设计工程, 2009, 17(3):98-100.
[3] 范明俊, 李宁, 赵乐军,等. 一种安全可靠性高的全新 IP 核保护方法[J]. 微电子学, 2007, 37(2):185-188.
[4] GUNGYSU T, MOLLER B, PAAR C, et al. Dynamic intellectual property protection for reconfigurable devices[C]. Kitakyushu: Field-Programmable Technology, 2008:169-172.
[5] 杨义先, 钮心析. 应用密码学[M]. 北京: 北京邮电大学出版社, 2005.

(收稿日期:2012-05-28)

作者简介:
董春国,男,1972 年生,本科,主要研究方向:电气工程。