

一种基于 SRAM 的 FPGA 的加密方法

吴其达, 吴皓威, 刘晓明, 欧静兰

(重庆大学 通信工程学院, 重庆 400044)

摘 要: FPGA 在现代电子系统设计中, 由于其卓越性能、灵活方便而被广泛使用, 但基于 SRAM 的 FPGA 需要从外部进行配置, 配置数据很容易被截获, 故存在安全隐患。总结了当前 FPGA 的加密方法; 提出了一种基于外部单片机的 FPGA 加密方法, 该方法中使用外部单片机配合 FPGA 产生了真随机数, 并利用随机数进行加密, 保护 FPGA 内部设计的知识产权; 最后给出了该加密方法的一个实例。实验结果表明, 该方法实现简单、使用灵活, 适用于成本敏感场合。

关键词: 现场可编程门阵列; STC 单片机; 随机数; 加密

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2008)10-0148-03

An Encryption Method of SRAM-Based FPGA

WU Qi-da, WU Hao-wei, LIU Xiao-ming, OU Jing-lan

(College of Communication Engineering, Chongqing University, Chongqing 400044, China)

Abstract: In the modern electronic system design, FPGAs are widely used because of its excellent capability and agile design. However, SRAM-Based FPGA need be configured outside, and the configuration data may be captured easily, which bring out security problem. Summarizes the current methods of FPGA encryption, and brings forward a new method of based external single-chip microcomputer FPGA encryption. This method produces real random number by SCM cooperating FPGA and adopts proper encryption algorithm to encrypt the random number, protect the intellectual property of the FPGA internal design. At last, show an example of the encryption. The experiment indicates that the method is implemented easily, used neatly, and suitable for cost sensitive occasion.

Key words: FPGA; STC single-chip microcomputer; random number; encryption

0 引言

FPGA 因其性能卓越、设计灵活, 在电子设备领域得到广泛应用, 但是基于 SRAM 的 FPGA 上电后, 需要从外部进行配置。在配置过程中, 任何人都可以轻易地监控 BIT 流, 并且克隆器件, 从而复制整个设计系统。因此, 在使用 FPGA 时, 如何有效地保护知识产权成为摆在 FPGA 制造商和开发者面前的难题之一。

目前, 业界已经有很多针对 FPGA 的加密方法:

1) FPGA 内置密钥。Xilinx 的 Virtex-II 和 Virtex-4 系列^[1]的高端 FPGA 中, 支持对配置数据流的加密操作。这样仅当 FPGA 中含有相同的密钥时, 这些数据流才可以工作。Altera 的 Stratix II 系列 FPGA 使用 AES(Advanced Encryption Standard)及 128 位非易

失密钥, 适用于对设计要求具有灵活性和保密性的应用场合, 该方案将不同的安全密钥设置在不同的 Stratix II 器件中, 可以进行配置文件加密, 使 IP 供应商能够跟踪确切的 IP 使用情况, 帮助用户保护其核心技术和信息, 防止被篡改, 实现了产品版本控制和定制。但是这种加密的方法对广泛使用的、对成本很敏感的应用场合来说不甚合适。

2) 外接加密芯片。文献[2]给出了一线存储器加密方式为 FPGA 提供安全控制和保护, 其中采用不可逆的 HASH 算法, 具有极高的雪崩效应。在这种加密方式中, 器件上电后, FPGA 从引导存储器中读取数据对自己进行配置, 配置完成后 FPGA 的微处理器功能被启动并进行认证工作。该加密算法需要占用 FPGA 大量的逻辑资源, 而且对加密芯片也有一定的要求, 使用起来有一定的局限性。

3) FPGA 内置引导存储器。基于 SRAM 的 FPGA 的不安全性来自于外挂的引导存储器, 所以有些 FPGA 公司将外部配置芯片集成到内部, 能提供单芯片的解决方案, 由于没有外接的引导器件, 启动时无需外部编程信号流, 从根本上解决了外部窥探 SRAM FP-

收稿日期: 2008-01-09

基金项目: 云南省重点科技项目(2003SABLB00A044)

作者简介: 吴其达(1981-), 男, 四川德阳人, 硕士研究生, 研究方向为计算机通信与测控、FPGA 设计与应用、加密技术等; 刘晓明, 教授, 博士后, 研究生导师, 研究方向为软件无线电、计算机测控、信号与图像处理等。

GA 编程信号流的安全隐患。例如, LATTICE 公司的 XP 系列, Actel 公司 40MX 系列等都采用了内部配置芯片。当前, 采用内部配置的 FPGA 芯片所占的市场份额并不大, 但是为 FPGA 知识产权保护提出了一个发展方向。

4) 外接单片机加密。文献[3]提供了一种基于单片机的 FPGA 加密方法, 但使用该方法生成的伪随机码序列固定, 故存在不安全因素。如果在 FPGA 系统上电后, 存储一定时间的伪随机序列; 然后用通过延长 DCLK 信号的周期, 降低伪随机码的传输速率, 即使没有获取全部的伪随机码, 也可以使 FPGA 长时间的正常工作。

文中针对 FPGA 在成本敏感的应用场合, 如消费类电子产品、民用工业产品中的应用, 提出了一种利用外接单片机的, 简单方便、保密性好的 FPGA 加密方法。

1 基于 SRAM 的 FPGA 的有效加密方法

由于 SRAM 工艺的 FPGA 上电时的配置数据是可以被复制的, 因此单独的一块 FPGA 芯片是无法实现有效加密的。FPGA 芯片供应商对位数据流的定义是不公开的, 因此无法通过外部的配置数据流信息推测内部电路。也就是说, 通过对 FPGA 配置引脚的数据进行采样可得到配置信息, 但也不能知道内部电路结构。如果在配置完成后使 FPGA 处于非工作状态, 利用另外一块保密性较强的单片机产生密码验证信息与 FPGA 进行通信, 仅在验证成功的情况下使 FPGA 正常工作, 则能有效地对 FPGA 进行加密^[4]。

文中采用了一种基于随机数的加密方法, 其原理结构如图 1 所示。随机码发生器是本设计的一个重要模块, 用来生成真随机码, 供加密算法模块使用。由于随机码需要输出至外部加密单片机, 在传输过程是可见的, 所以单片机必须对随机码进行必要的处理, 这就是加密算法模块的作用: 把随机码作为初相, 生成加密序列。验证模块把 FPGA 内部生成的加密序列与单片机输入的加密序列进行比较, 控制 FPGA 用户设计部分是否开始工作。

在上述方法中, 为了实现可靠的加密, 首先需要选择一款保密性能好的单片机或 CPU。这里的“保密性能好”指的是该单片机物理特性好, 根本无法破解该单

片机, 或者破解该单片需要支付高昂的解密费, 从而使仿制者望而却步。

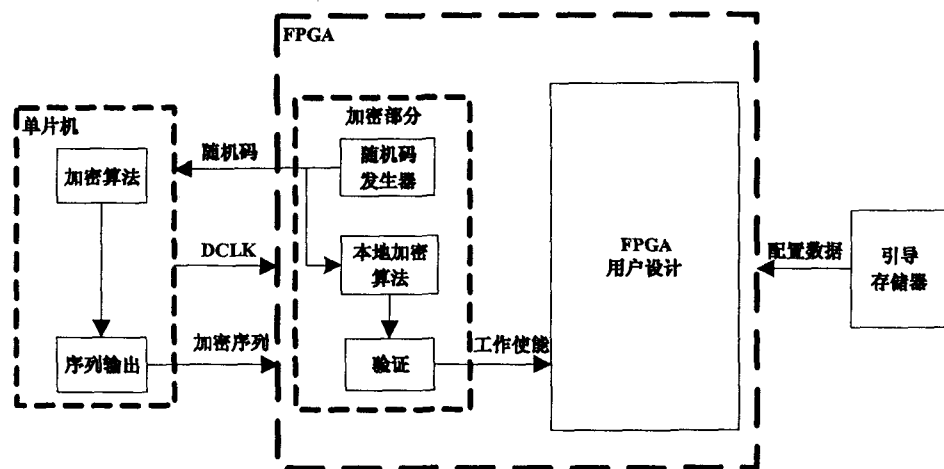


图 1 FPGA 加密原理图

其次, 电路中生成的随机码是真随机码^[5], 由硬件产生, 每次上电工作生成的数没有任何规律可循。它取决于以下因素:

- 1) FPGA 和单片机的振荡源不相关;
- 2) 利用高频率时钟信号采样低速信号, 且两信号频率相差在 100 倍以上;
- 3) FPGA 和单片机的配置时间不一致, 而且受温度和工作电压的影响。FPGA 的配置时间一般在几十至几百毫秒, 而单片机的配置时间根据器件的不同而不同。由于器件每次开始工作时, 电源电压和温度都不可能完全相同, FPGA 和单片机配置时间每次都有微小的差异。如果 FPGA 使用较高的计数频率, 就可以检测出这个时间上的微小差异, 生成真随机码。

最后, 需要一套合适的加密算法。由于采用了随机数, 每次都需要把随机数送往外部的加密芯片, 在传输的过程中, 原码是可见的, 故必须选择一种方式对原码进行处理。文中推荐了两种算法: 简单的线性码高阶 GOLD 序列和 AES^[6]。

Gold 序列是 R·Gold 提出了一种基于 m 序列的码序列。这种序列有较优良的自相关和互相关特性, 构造简单, 产生的序列数多。其线性移位寄存器的特征多项式 $g(x) = f_1(x)f_2(x)$ 中, 若 $f_1(x)$ 是 n 阶本原特征多项式, 生成周期为 $N_1 = 2^n - 1$ 的最大长度序列, $f_2(x)$ 是 m 阶本原特征多项式, 生成周期为 $N_2 = 2^m - 1$ 的最大长度序列, 那么 $g(x)$ 生成的序列周期 $N = \text{LCM}(N_1, N_2)$, 即 N 是 N_1, N_2 的最小公倍数。如果 $f_1(x), f_2(x)$ 是 n 阶的不同本原特征多项式, 那么 $g(x)$ 生成的序列周期也是 $N = 2^n - 1$ 。而且 Gold 序列的生成多项式很复杂, 不可能通过简单的方法计算出来, 提高程序的安全性。

AES 是美国国家标准技术研究院 (NIST) 颁布的加密标准。AES 算法能够使用 128、192 和 256 位的密钥来实现 128 位数据块的加密和解密, 从而保护电子数据。AES-128 能在多达 3.4×10^{38} 个独特密码键中任挑一个来加密位流。这样, 每秒能破解一百万个加密键并可用于设计的精密黑客程序 (这已是非常高的并发算法能力了) 也需要 1×10^{25} 年 (即千万个万亿年) 才能找到 AES-128 生成的那个加密键。

在上述的算法中, Gold 序列的实现简单、保密性好, 一般的单片机都可以实现, 适用于价格比较敏感的场所, 而 AES 是一种高级加密算法, 对外部的加密芯片有一定的要求, 用户可以根据自己的需要选用。

由于采用了随机数, 每次加密算法的初始相位都不相同, 其加密算法产生的结果是不可预测的, 通过简单方法破解是不可能实现的。而且在实际应用过程中, 用户可以根据不同的需要, 改变加密算法, 从而增加破解的难度和周期, 保证了加密的可靠性。

2 应用举例

下面给出了一个采用上述 FPGA 加密方法的实例: 单片机选用宏晶公司的 STC 单片机; FPGA 选用 Altera 公司的 Cyclone II 系列的 EP2C5; 加密算法选用 Gold 序列加密, 其本原特征多项式 $f_1(x)$, $f_2(x)$ 分别为 10 阶、11 阶。

STC 单片机是由美国设计, 国内宏晶公司贴牌生产的, 这个芯片设计的时候就吸取 51 系列单片机很容易被破解的教训, 改进了加密机制。STC 单片机出厂的时候就已经完全加密, 用户程序是 ISP/IAP 机制写入, 编程的时候是一边校验一边写, 无法读出命令, 因此抗破解的能力很强。

Altera 公司的 Cyclone II 系列 FPGA 最大配置时间为 $RBF(\text{Raw Binary File}) \times (\text{最大时钟周期} / 1 \text{ 比特})$, 以 EP2C5 为例 ($1\,223\,980$ 比特的未压缩数据), 使用 40MHz 的振荡器, 时钟最小频率为 20MHz (50ns) 其最大配置估计时间为 $1\,223\,980 \text{ 比特} \times (50 \text{ 纳秒} / 1 \text{ 比特}) = 61.2 \text{ 毫秒}$, 一块单片机的配置时间很短 (使用内部振荡电路), 而且 PIC 的配置时间还要受当时的工作电压和温度的影响。由于器件每次开始工作时, 工作电压和温度都不可能完全相同, FPGA 和 PIC 配置时间的差值每次都有微小的差异, 而且 FPGA 振荡器产生的时钟源与 PIC 单片机内部振荡电路产生的时钟不相关, 且 FPGA 的计数频率很高, 可以检测出这个时间上的微小差异, 以此生成真随机码。对上述随机码发生电路进行了 200 次测试, 测试结果显示每次产生的

随机码均不相同。

Gold 序列的生成多项式, 如图 2 所示, 其中 $f_1(x) = x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $f_2(x) = x^{11} + x^2 + 1$ 。则 $g(x)$ 生成的序列周期是 $N = (2^{11} - 1) \times (2^{10} - 1) = 2^{21}$, 前面产生的真随机数用作 Gold 序列发生器的初相。在此例中 Gold 序列的阶数较少, 若采用高阶 Gold 序列, 例如 40 阶其最大序列的周期为 $2^{40} = 10^{12}$, 将所有的序列截获并存储就需要 1000Gb 的存储空间, 若码速率为 50kbps , 捕获时间将长达 5555 小时。Gold 序列具有很好的保密性, 用户还可以根据需要, 改变反馈系数, 增加寄存器阶数, 从而增加加密算法的安全性。

FPGA 加密流程如图 3 所示。

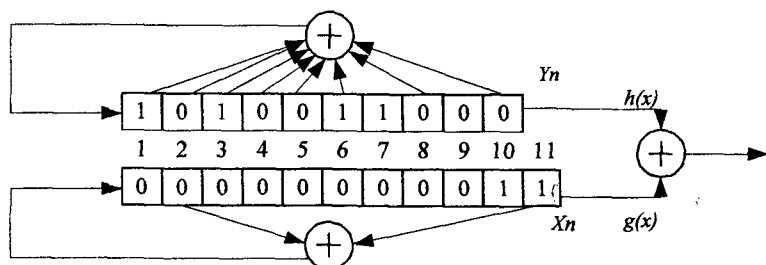


图 2 Gold 序列生成器

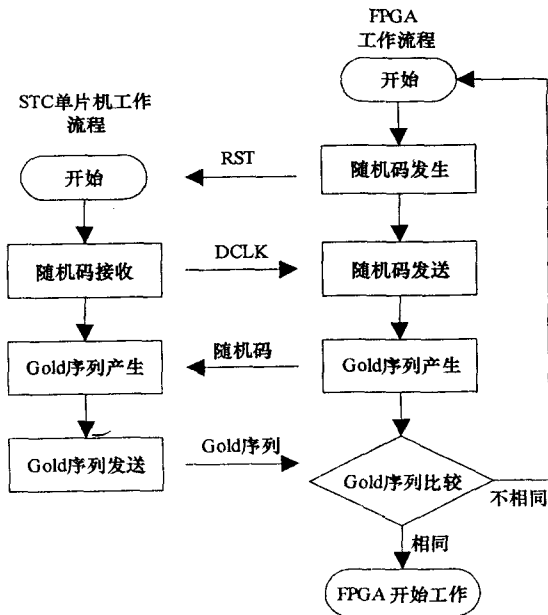


图 3 FPGA 加密工作流程

单片机配置完成后, 延时一个随机时间, 再发送一个高电平给 FPGA。而 FPGA 配置完成后立即开始高频计数, 利用这个到来的上升沿停止计数, 生成真随机码。FPGA 把生成的随机码发送给单片机。单片机把接收到的随机码作为 Gold 序列的初始相位, 生成 Gold 序列, 并把生成的 Gold 序列发送给 FPGA。FPGA 内

(下转第 154 页)

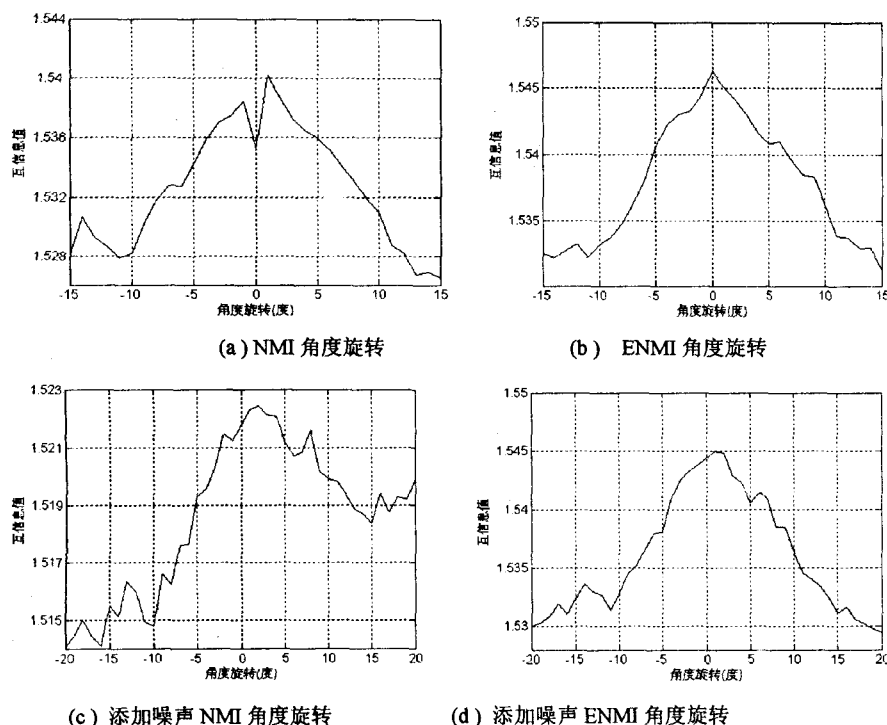


图 3 采用 NNI 和 ENMI 角度配准曲线对比

表 2 添加噪声配准结果比较

基于邻域信息的互信息			传统互信息		
旋转	x 轴平移	y 轴平移	旋转	x 轴平移	y 轴平移
2.80	33	29	2.60	34	29
3.20	33	28	2.70	35	29
3.20	35	30	2.80	35	32
3.40	34	28	3.40	34	27
3.00	34	31	1.70	33	34

3 结束语

文中提出了一种基于邻域信息的互信息配准算法,该算法既利用了图像的灰度互信息又充分利用了

图像像素的空间信息,通过大量实验证明在红外与可见光图像配准中采用该算法与采用传统的互信息配准算法相比配准曲线更加光滑,从而在目标参数寻优过程中更易于找到极值,提高了配准精度和抗噪能力。

参考文献:

- [1] Collignon A, Maes F, Delaere D, et al. Automated multimodality medical image registration using information theory [C]//Proc 14th Int Conf Information Processing in Medical Imaging (IPMI, 95). Ile de Berder, France: IEEE Press, 1995: 263-274.
- [2] Josien P, Antoine J, Max V. Image registration by maximization of combined mutual information and gradient information[J]. IEEE Trans on Medical Image, 2000, 19(8): 809-814.
- [3] Rueckert D, Clarkson M J, Hill D L G, et al. Non-rigid registration using higher-order mutual information [C]//Proc SPIE Medical Imaging 2000: Image Processing. San Diego, CA: [s. n.], 2000: 438-447.
- [4] Studholme C, Hill D L G, Hawkes D J. An overlap invariant entropy measures of 3D medical image alignment[J]. Pattern Recognition, 1999, 32(1): 71-86.
- [5] 姜晓彤, 罗立民, 赵正旭. 一种改进的基于互信息和梯度特征的图像配准方法研究[J]. 仪器仪表学报, 2006, 27(9): 1141-1146.

(上接第 150 页)

部也有同样的 Gold 序列生成电路,把接收到单片机发来的 Gold 序列与内部生成的 Gold 序列进行比较。若相同, FPGA 用户设计开始工作;若不相同,则 FPGA 用户设计不工作。

3 结束语

文中提出了一种针对基于 SRAM 的 FPGA 进行加密的方法,该方法简单方便、保密性好、容易升级,适用于价格敏感的场所。在对外部单片机的选择方面,除了 STC 单片机外,也可以采用其他保密性好的单片机对 FPGA 进行加密;在加密算法方面,由于 Gold 序列是由 m 序列产生,具有一定的局限性,还可以使用安全性更高的 AES,提高加密算法的可靠性。

参考文献:

- [1] Virtex-4 系列概述[EB/OL]. 2007-01-23. www.xilinx.com.
- [2] XILINX®FPGA IFF Copy Protection with 1-Wire SHA-1 Secure Memories[M]. Dallas: [s. n.], 2006.
- [3] 刘晓明, 谢明钦, 王 军. 用单片机实现 SRAM 工艺 FPGA 的加密应用[J]. 单片机与嵌入式系统应用, 2003(7): 17-20.
- [4] Ray S. A Whitepaper on SRAM FPGA security[EB/OL]. 2003-02. http://www.fpga.com.cn & www.pld.com.cn.
- [5] 肖俊安, 周祖德. 高效真随机序列生成方法的研究[J]. 计算机工程与应用, 2006(16): 1-3.
- [6] Daemen J, Rijmen V. 高级加密标准(AES)算法——Rijndael 的设计[M]. 北京: 清华大学出版社, 2003.