

利用 LUT 替换的 FPGA 保护数字水印技术

聂廷远, 刘海涛, 周立俭, 李言胜

(青岛理工大学 通信与电子工程学院, 山东 青岛 266033)

摘 要: 提出一种新的基于查找表替换的 IP 核数字水印技术, 利用基于存储式逻辑阵列块(Memory Logic Array Block, MLAB)的 RAM 结构替换原设计文件中的查找表, 在其中添加水印数据. 使用此方法使嵌入的水印可以避免被优化工具删除, 提高了数字水印的安全性. 实验表明, 此方法嵌入数字水印的效率高, 资源开销较低, 优于其它基于查找表的数字水印方法.

关键词: IP 核保护; 数字水印; FPGA; LUT

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2013)01-0021-03

LUT Replacement Based FPGA Watermark Protecting Technique

NIE Ting-yuan, LIU Hai-tao, ZHOU Li-jian, LI Yan-sheng

(Communication and Electronic Engineering Institute, Qingdao Technological University, Qingdao 266033, China)

Abstract: A new watermarking technique based on LUT replacement is proposed. Firstly, the watermarks are embedded into the memory logic array block(MLAB). Then, use a MLAB-based RAM to replace the corresponding LUT of original IP core. Because of the property of MLAB, the signatures embedded in MLAB can be preserved from the optimization process of EDA tools. The experimental results show that the method is more effective. The overheads and timing penalty of watermarking are very low, compare to other LUT-based watermarking technique.

Key words: intellectual property protection; watermarking; FPGA; look-up table (LUT)

1 引言

当前, SoC(System on Chip)技术已成为集成电路设计的主流, IP(Intellectual Property)核复用成为 SoC 设计中的重要技术, 如何保护 IP 核已成为集成电路产业发展中要解决的迫切问题之一^[1].

数字水印技术是一种 IP 保护的重要手段, 其原理是将 IP 模块作为水印载体, 在电路设计中隐藏特定的数字标记信息, 通过对数字水印的检测和鉴别, 来证明其产权归属或跟踪侵权^[2].

文献[3]阐述了基于 FPGA 的水印保护方法. 文献[4]提出了基于 FPGA 的数字水印技术, 基本原理是将加密的水印签名嵌入到未使用的查找表(Look Up Table, LUT)中. 文献[5-7]又做了改

进, 这种方法添加水印的安全性进一步得到提高, 但是需要一定的面积和时间开销.

本文提出一种新的基于 LUT 替换的数字水印技术, 利用一种新型的存储式逻辑阵列块(Memory Logic Array Block, MLAB), 在其中添加水印数据, 用这些 MLAB 替换原设计文件中已使用的 LUT, 并在 IP 核中嵌入数字水印. 该方法嵌入数字水印信息量大, 安全性高, 资源开销较低, 优于以上基于 LUT 的数字水印方法.

2 基于 LUT 替换的 FPGA 数字水印方法

2.1 基于 LUT 替换的数字水印嵌入原理

FPGA 器件的可编程资源主要由逻辑单元(Logic Elements, LE)构成, 在 Altera 的 Stratix III

收稿日期: 2012-05-16; **修回日期:** 2012-06-13

基金项目: 教育部留学回国人员科研启动基金资助项目; 山东省自然科学基金(ZR2009GL007); 山东省高等学校科技计划项目(J09LG10)

器件^[8]中,一个 LE 主要由一个 6 输入查找表、一个可编程触发器、一个全加器等组成. 查找表本质上就是一个 RAM,一个 6 输入的查找表可以看成是一个有 6 位地址线的 64×1 的 RAM. 设计者通过原理图或 HDL 语言描述了一个逻辑电路以后,开发软件会自动计算逻辑电路的所有可能的结果,并把结果事先写入查找表,这样每输入一个信号进行逻辑运算就等于输入一个地址进行查表,找出地址对应的内容,然后输出.

Lach 等人提出的基于 LUT 的数字水印嵌入方法,其原理是使用 IP 核设计中存在的大量未使用的 LUT,在其中嵌入水印,连接到原始设计的其它 LUT,加以隐藏. 这种方法水印嵌入简单,但是安全性较差,增加的 LUT 只是简单的跟原设计相连,盗用者利用逆向工程很容易找到这些 LUT,将之去除. 尽管后续研究对这种方法进行了改进,但在本质上并没有提高其安全性.

在完成设计之后,大量已使用的查找表存在闲置的输入端口,也即查找表内存在大量的空余存储空间,这些存储空间可以利用,添加数字水印. Schmid 等人首先提出此类方法,在网表层将水印数据添加到查找表内,相比在其它设计层添加水印,具有操作简单等优点.

值得注意的是,如果通过直接修改网表文件中的查找表,经过 FPGA 软件编译之后,添加的水印数据会被编译器中的优化工具自动修改乃至删除,使保留的数字水印不完整. 因此我们利用 Stratix III 器件^[8]中新增加的一种 MLAB 结构,添加数字水印. LAB 和 MLAB 是 Stratix III FPGA 中的共存对,MLAB 可用作普通的 LAB,也可以配置为双端口静态随机存储器. Stratix III 器件中一半的 LAB 可以配置为 MLAB,MLAB 可以放在器件中的任何位置,使用灵活.

在网表设计文件中,大量查找表存在闲置输入端口. 因而可以在设计综合之后的网表文件中,随机选择具有多个输入端闲置的 LUT,将这些 LUT 的输入端替换为 RAM 的地址线,输出端替换为 RAM 的一位输出. 然后将 RAM 的其它地址线设置为高电平,数据输入端 DATA 和写使能端 WREN 设置为低电平. 最后在 RAM 的初始化文件中写入 LUT 数据与水印数据. 水印嵌入之后,对设计功能无任何影响,而且产生极低的面积开销和时间开销,水印存在于 MLAB 中,盗用者无法找到水印位置,且 MLAB 可以抵御优化操作,安全性较高.

图 1 给出了一个数字水印嵌入的实例,6 输入查找表可以存储 $2^6 = 64$ 比特的数据,但是若只有两个输入端,如图 2 所示,查找表的逻辑功能为“ $\text{out} \leftarrow e \text{ and } f$ ”,其中存储的数据实际上只有最后四位“0001”,只占用查找表 4 比特的存储空间. 若将网表文件中的 LUT 替换为基于 MLAB 的具有 6 位地址线的 64×1 的 RAM,则可以在未利用的存储空间嵌入 60 比特的水印数据.

a	0	0	0	0	1	1	1	1	1
b	0	0	0	0	1	1	1	1	1
c	0	0	0	0		1	1	1	1
d	0	0	0	0	0	0	0	1	1
e	0	0	1	1	1	1	0	0	1
f	0	1	0	1	0	1	0	1	0
out					0 0 0 1				

待加水印位置 $\text{out} \leftarrow e \text{ and } f$

图 1 基于 MLAB 的 RAM 添加水印实例

2.2 基于 LUT 替换的数字水印嵌入流程

基于 LUT 替换的数字水印嵌入流程如图 2 所示,步骤如下:

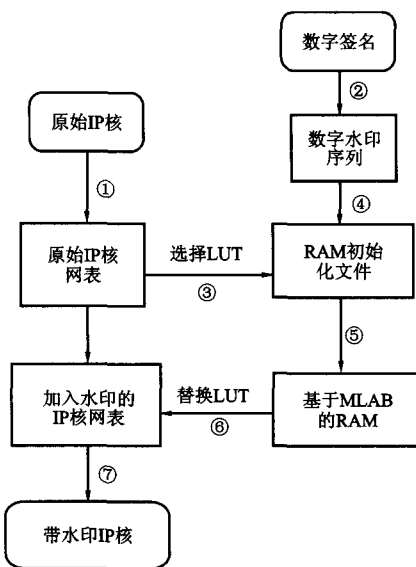


图 2 水印嵌入流程

①由原始 IP 核设计文件经过综合工具得到网表文件;

②将原始的签名信息经过编码、加密等操作后生成待添加的水印序列;

③根据水印序列的大小,在网表文件中随机地选择若干个 LUT,并读取其中存储的数据;

④对应所选择的 LUT,生成若干基于 MLAB 的 RAM 模块,将其网表文件中的地址线配置为对应 LUT 的输入端,输出配置为 LUT 的输出,其它地址线设置为高电平,数据输入端 DATA 和写使能

端 WREN 设置为低电平;

⑤生成 RAM 的初始化文件,将选择的 LUT 存储的数据和待添加的水印序列写入到初始化文件中;

⑥将原始 IP 核的网表文件的 LUT 替换为相应的基于 MLAB 的 RAM;

⑦将替换好的网表文件重新编译,生成带有水印的 IP 核设计.

3 实验与结果分析

实验在 Altera 的 Quartus II 开发平台上进行,综合工具采用 Synplify,FPGA 器件选用 Stratix III 系列. 我们选用三个普通的开源 IP 核进行测试:DES,CAN,AES. 其中 DES 和 AES 为加密算法 IP 核,CAN(Controller Area Network)为串行通信协议控制器. 三种 IP 核的特性如 LUT 数量、最小时钟周期、寄存器数量,如表 1 所示.

表 1 实验 IP 核特性			
IP 核	LUT	最小时钟周期(ns)	寄存器
DES	444	2.508	190
CAN	1101	3.694	669
AES	1583	5.388	807

为了衡量嵌入水印后 IP 核设计的开销,我们分别在三种 IP 核中嵌入 60 比特、120 比特和 240 比特的水印数据,并计算 LUT、寄存器嵌入前后的增加百分比,和最小时钟周期嵌入前后的增加百分比,实验数据如表 2、表 3、表 4 所示.

由对比数据可以看出:LUT 的增加基本上是由于加入了嵌入水印的 MLAB,变化范围较小,从 0.27%到 4.28%,在可以接受的范围之内;由于使用基于 MLAB 的 RAM 结构替换了原设计中的 LUT,对设计的时序优化有一定的影响,最小时钟周期有一定程度的增加,DES 核嵌入 240 位水印时最大,为 9.20%;寄存器总体上增加也非常小,在 DES 核嵌入 240 位水印时最大,为 6.32%. 由于使用了 Stratix III 的 MLAB 结构,使水印嵌入的效率大大提高,而且增加的资源开销较低.

因为 DES 核较小(LUT 仅为 444),在添加较大数量的数字水印时,会给设计带来影响. 因此,设计者在进行 FPGA 设计保护时,应根据 IP 模块的大小,合理设置数字水印的大小,使其性能不会产生太大的影响.

Schmid 等人使用的方法,在嵌入 320 位水印数据的情况下,LUT 增加量-1.28%~4.97%,最小

时钟周期 10.11%~39.19%^[7]. 本文的方法使用基于 MLAB 的 RAM 替换 LUT 嵌入水印,可以充分利用 MLAB 的存储特性,不仅资源开销控制在一定范围之内,而且最小时钟周期的变化范围也可以得到很好的控制.

表 2 DES 核嵌入水印后资源开销增加对比			
水印大小(bit)	60	120	240
增加 LUT(%)	1.80	0.90	4.28
增加时钟周期(%)	-0.32	6.78	9.20
增加寄存器(%)	0	3.06	6.32

表 3 CAN 核嵌入水印后资源开销增加对比			
水印大小(bit)	60	120	240
增加 LUT(%)	0.73	0.73	0.27
增加时钟周期(%)	1.57	-2.14	0.62
增加寄存器(%)	0.75	0.60	0.30

表 4 AES 核嵌入水印后资源开销增加对比			
水印大小(bit)	60	120	240
增加 LUT(%)	1.71	1.64	1.90
增加时钟周期(%)	2.97	6.22	3.93
增加寄存器(%)	1.86	2.23	2.23

4 结束语

本文提出基于 LUT 替换的数字水印技术,将水印数据嵌入到一种新型的存储式逻辑阵列块 MLAB 中,利用基于 MLAB 的 RAM 结构替换原设计文件中已使用的 LUT. 相对于其它方法,利用结构替换使嵌入的水印可以避免被编译器中的优化工具删除,确保了水印的鲁棒性,MLAB 的使用提高了水印的嵌入效率,使资源和时序开销控制在较小的变化范围内,提高了数字水印的安全性.

参考文献:

[1] 谢学军,邱善勤. IP 在中国的现状与未来之路[J]. 半导体技术,2005,30(6):1-4.

[2] 李东晓,郑伟,张明. IP 芯核水印技术研究进展[J]. 电路与系统学报,2007,12(4):85-92.

[3] 苗胜,戴冠中,慕德俊,等. 基于 FPGA 的 IP 核水印保护方法[J]. 微电子学与计算机,2007,24(3):30-33.

[4] John Lach, William H, Mangione-Smith, et al. Signature hiding techniques for FPGA intellectual property protection[C]//ICCAD'98: Proceedings of the 1998 IEEE/ACM international conference on Computer-aided design. New York, NY, USA, 1998:186-189.

虽然改进后的算法在时间上比原算法要长,但是在网络路由准确性上却比原算法高出很多.对于云计算而言,时间上的代价差距是可以忽略的,而以此代价换来的资源调度中路由的准确性却是非常值得的.

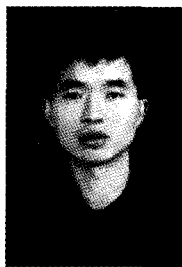
参考文献:

- [1] 范杰,彭舰,黎红友.基于蚁群算法的云计算需求弹性算法[J].计算机应用,2011,31(1):1-7.
- [2] 华夏渝,郑骏,胡文心.基于云计算环境的蚁群优化计算资源分配算法[J].华东师范大学学报,2010,1(1):127-134.
- [3] Tian Wenhong, Zhao Yong, Zhong Yuanliang, et al. Dynamic and integrated load-balancing scheduling algorithm for cloud data centers[C]//Cloud Computing and Intelligence Systems(CCIS), IEEE International Conference on. Taiwan, 2011:311-315.
- [4] 史恒亮,白光一,唐振民,等.基于蚁群优化算法的云数据库动态路径规划[J].计算机科学,2010,37(5):143-145.
- [5] Zhe Cong, Bart De Schutter, Robert Babuska. A new ant colony routing approach with a trade-off between system and user optimum[C]// 2011 14th International

al IEEE Conference on Intelligent Transportation Systems. Washington, DC, USA, 2011:1369-1372.

- [6] Yong Wu, Lin Ma, Jing Yang. Ant colony algorithm for optimal resources configuration of equipment maintenance support[D]. Department of System Engineering of Engineering Technology Beijing University of Aeronautics and Astronautics, 2011:793-795.

作者简介:



刘伯红 男,(1973—),硕士,副教授.研究方向为分布式系统、云计算.

赵浚尧 男,(1986—),硕士研究生.研究方向为云计算及其应用.

王刚 男,(1987—),硕士研究生.研究方向为云计算及其应用.

阎英 女,(1977—),硕士,副教授.研究方向为宽带网络技术.

(上接第23页)

- [5] John Lach, William H, Mangione-Smith, et al. Robust FPGA intellectual property protection through multiple small watermarks[C]// DAC'99: Proceedings of the 36th annual ACM/IEEE Design Automation Conference. New York, NY, USA, 1999: 831-836.
- [6] Debasri Saha, Susmita Sur-Kolay. Fast robust intellectual property protection for VLSI physical design [C]//ICIT'07: Proceedings of the 10th International Conference on Information Technology. Washington, DC, USA, 2007:1-6.
- [7] Moritz Schmid, Daniel Ziener, Jürgen Teich. Netlist-level IP protection by watermarking for LUT-based FPGAs[C]// Proceedings of IEEE International Conference on Field-Programmable Technology. Taipei, Taiwan, 2008:209-216.
- [8] Altera. com. cn. Stratix III device handbook[EB/OL] (2012-06-10). http://www.altera.com.cn/literature/hb/stx3/stratix3_handbook.pdf.

作者简介:



聂廷远 男,(1971—),博士,副教授,IEEE会员.研究方向为VLSI CAD系统的设计、VLSI芯片知识产权保护数字水印技术、信息安全等.

刘海涛 男,(1988—),硕士.研究方向为数字水印技术、信息安全.

周立俭 女,(1970—),博士,副教授.研究方向为图像处理与模式识别等.

李言胜 男,(1973—),副教授.研究方向为高速模拟微电子集成技术、IP保护信息安全技术、高频信号电路设计及实装技术等.