DOI：10.19816/j.cnki.10-1594/tn.2020.01.095

IP保护方法研究进展*

张 伟[1]，冯建华[1,2,3]

（1.北京大学微纳电子学系 北京 100871；2. 北京大学软件与微电子学院 北京 100871；
3.北京大学（天津滨海）新一代信息技术研究院 天津 300450）

摘 要：电子器件生产成本的增加和集成电路设计方法的改变已导致微电子工业中的新兴威胁，例如伪造、非法复制、反向工程和盗窃，IP保护已经成为一个重要的研究课题。系统概述了各种主流的IP保护方法，包括加密与许可证机制、数字指纹、数字水印、硬件计量、硬件混淆等，重点介绍了基于约束、附加、模块、功率的数字水印方法的研究进展，也介绍了几种最新的IP保护方法，提出了未来IP保护可能的发展方向。

关键词：IP核；硬件安全；数字水印；硬件计量

中图分类号：TN492 **文献标识码**：A **国家标准学科分类代码**：510

Research progress on IP protection techniques

ZHANG Wei[1], FENG Jianhua[1,2,3]

（1. Institute of Microelectronics, Peking University, Beijing 100871, China;
2. School of Software & Microelectronics, Peking University, Beijing 100871, China；
3. Peking University Information Technology Institute (Tianjin Binhai), Tianjin 300450, China）

Abstract：The increasing production costs of electronic devices and changes in the design methods of integrated circuits has led to emerging threats in the microelectronics industry such as counterfeiting, illegal copying, reverse engineering and theft. IP protection has become an important research topic. It systematically summarizes various mainstream IP protection techniques in the paper, including encryption and license mechanisms, digital fingerprints, digital watermarks, hardware metering, hardware obfuscation, etc., and focuses on the research of constraint, addition, module, and power-based digital watermarking techniques. The progress also introduced several latest IP protection techniques, and proposed the possible development direction of IP protection in the future.

Keywords：IP core; hardware security; digital watermark; hardware metering

0 引 言

随着集成电路产业的发展，IP核（intellectual property core）复用成为系统芯片（SOC）、专用集成电路（ASIC）和现场可编程门阵列（FPGA）设计的重要方法。在IP核复用得到广泛应用的同时，如何使IP核不被非法盗用成为行业亟待解决的关键问题。1996年，成立了虚拟插件接口联盟（VSIA），以通过建立采用IP的标准（VSIA也称为虚拟组件）来显著提高半导体行业的设计生产率。VSIA确定了6个挑

*基金项目：国家自然科学基金（61672054, 61176039）项目资助
张伟，硕士，主要研究方向为IP保护。E-mail：zhangweixmu@163.com
冯建华（通信作者），副教授，主要研究方向为VLSI测试和可测试性设计、硬件安全。E-mail：fengjh@pku.edu.cn

战,并为每个挑战建立了开发和工作组(DWG),其中,IP保护(IPP)是颇具挑战的技术之一。IPP DWG创建于1997年,目标是:(1)使IP提供商能够保护其IP免受未经授权的使用;(2)保护用于生产和交付IP的所有类型的设计数据;(3)检测IP的使用;(4)跟踪使用IP的数量[1]。

为了达到IP保护目标,学术界与工业界均开展了广泛研究。其中,VISA关于IP保护的白皮书和其物理标记标准[1]已经被半导体厂商和EDA工具提供商广泛采纳和使用。IPP DWG在2000年发布的第一份文件中,确定了3种保护IP的方法:(1)采用威慑方法,IP所有者可以通过使用适当的法律手段阻止侵权者盗用IP;(2)采用保护方法,所有者尝试防止未经授权使用IP;(3)采用检测方法,所有者可以检测并跟踪合法和非法使用IP的情况[2]。常用的威慑手段包括专利、版权、合同、商标和商业秘密。保护机制采用诸如加密、许可协议、专用硬件或化学药品之类的手段来防止未经授权访问IP。在检测方法方面,IPP DWG建立了2个IP保护标准,一个是针对硬IP的物理标记标准,另一个是针对软IP的物理标记标准。这些标准在行业中采用时,可提供一种方便的方式来跟踪IP并检测IP的使用(IP保护的最后2个目标)。

针对IP核设计的各个阶段与流程,学术界与工业界都提出了大量关于IP保护机制的想法与建议[2-9, 10,11,12-15]。一般而言,工业界的研究集中于IP核的版权认证和合法使用的追踪,采用的方法主要是检验、版本更新与版权合法性报告等。而学术界的研究更多的是着眼于IP保护与检测的技术(例如数字水印和数字指纹等),其中少有被半导体厂商与EDA工具提供商应用。这个有趣的现象给了我们从不同的角度去思考IP版权保护这个相同问题的机会,同时比较这些方法各自的优缺点。

近年来IP保护方法主要包含“保护”与“检测”2个方面。保护主要针对IP核被非法复用前进行处理,通过加密和许可证机制阻止IP核的非授权使用。检测是属于非法复用后的处理办法,是在IP核被非法使用以后进行版权证明的一种技术手段。数字指纹是IP核特性的提取,而数字水印则主要是设计人员后期加工形成。目前,通过数字水印技术对IP核进行辅助的版权保护成为了学术界研究的热点。数字水印其实也是通过产权认证的方式对IP盗用者进行法律威慑,成为检测跟踪侵权行为的法律依据,本身无法阻止IP核的盗用行为。

本文系统地概述了各种主流的IP保护方法,包括加密与许可证机制、数字指纹、数字水印、硬件计量、硬件混淆等,重点介绍了基于约束、附加、模块、功率4种类型的数字水印的研究进展,也介绍了几种最新的IP保护方法,最后为结论。

1 加密与许可证机制

研究者最容易想到的一种IP保护方法就是通过EDA工具对IP核源文件进行加密处理,是用户在加密文件上进行操作处理而不修改源文件。这种加密机制使用户能够在对IP内部模块一无所知的情况下使用IP,采用IP核进行集成电路的设计。这种加密机制应该同时支持多种EDA工具以让用户完成高层次设计到仿真验证、布局布线的一系列过程。在这里IP核被当成一个“黑盒子”交付给用户。

加密的方法一定程度上防止了IP核的盗用但也存在以下几个严重的问题:

(1)EDA工具的后门隐患。为了解决EDA工具或者IP核内部的故障,所以EDA工具都保有对加密数据处理的另一套办法,即所谓的“后门”。

(2)bug追踪困难。由于加密的特殊性,当设计人员在系统仿真出现问题以后很难判断问题的原因是由EDA工具还是IP核本身,或者设计本身与IP核连接的错误造成。

(3)EDA工具提供商信任度问题。IP核加解密方法全部依赖于EDA工具提供商,设计者必须充分信任和依赖EDA工具的提供商。

(4)加密机制无法阻止反向工程的侵权行为。另外一种加密的方法是针对EDA工具本身或者IP核的算法进行加密[9],这种方法类似传统的基于加密和许可证的软件保护机制。由于缺乏许可证协议的强制实行和加密协议的安全漏洞,这种方法也无法提供给IP核完全有效的保护。例如,一个设计者非法利用EDA工具或者相关的算法设计出来一个电

路,很难从这个电路证明设计者的EDA工具与算法是否是合法获得的。因为IC设计者可以说是从其他的EDA工具与算法那里获取的。此外,诸如IBM提出的基于需求的芯片验证设计协作平台等在线协作设计框架[16-17]的搭建给EDA工具更多被不恰当使用的空间和机会。考虑到EDA工具与相关算法对电路设计的重要性,相关工具与算法的保护亟待解决。

2 数字指纹

数字指纹也称为被动水印,是利用IP核固有的一些已经存在的特性。这种方法的特点是不同的用户会得到不同的指纹IP版本,指纹嵌入到IP中不易被轻易移走。例如Lach等[7]首先提出以划分为基础的版权保护方法。当IP购买者向IP版权所有者购买IP时,IP所有者为设计的每一部分分配一种实现形式,再把这些部分组合匹配在一起提供给购买者,对不同部分的每一小部分实现不同的形式。这种方法的不足之处是每个IP模块都必须有独立的结构,增加了设计的代价。

Caldwell等[18]提出了一种基于递增迭代优化的指纹技术。利用电路设计中的SAT原理。首先,给定初始化实例,其中包含有IP提供者的水印信息,从头开始优化生成初解 S;第二,对应第 j 个用户将其指纹 F_j 加到 I_0,创建带有指纹信息的实习 I_j;最后,从上一个用户的解 S_j-1 出发,应用递增优化为 I_j 生成新的带有指纹的解 S_j。本方法相对于Lach的方法开销更低,鲁棒性更好。

另外还有研究者提出“噪声指纹”技术,它是一种类似数字指纹的被动保护方法。主要原理是利用电路的改动在硅衬底上面产生特殊的噪声信号,对输入信号和电路实现等细节处理,把噪声信号作为版权鉴别的标记。

总的来说,数字指纹方法局限性在于鲁棒性太差。数字指纹不带有IP所有者、IP命名等有用信息,对IP核的简单修改就会产生新的指纹,不利于IP核的复用。

3 数字水印

数字水印技术是一种将特制的不可见标记利用数字内嵌的方法隐藏的图像、声音、视频等数字内容中由此来确定版权拥有者和认证数字内容来源,识别购买者。确认所有权认证和跟踪侵权行为。数字水印包括水印生成、水印嵌入和水印恢复3部分,如图1所示。水印的生成过程就是在密钥 K 的控制下,有产权信息、认真信息、保密信息 m,生成适合于嵌入到原始载体 x 中的水印 w 的过程。

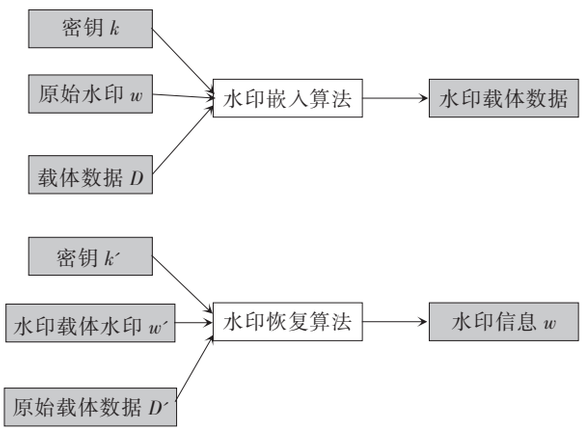

图1 水印嵌入与水印恢复

Fig.1 Watermark embedding and watermark recovery

如图2所示,数字水印方法的主要挑战在于尽量不影响原电路性能的基础上,开发一种难以破解的方法和工具。同时由于IP核分成了软核、固核、硬核这3大类,差别巨大,对于不同类型的IP核,需要研究相对应的适用方法。

由于IP核主要应用于厂商的设计复用,所以对水印技术有以下6个方面的具体要求:

(1)低开销。加入水印的代价与整个设计相比很小或者可以忽略。

(2)高可信度。为证明IP核的版权归属,水印的设计要很独特,与其他设计重合几率低。

(3)性能影响小。嵌入水印不改变IP核的基本逻辑功能,对面积、延时等影响可以忽略。

(4)检测方便。水印嵌入IP核之后能够有效的提取跟踪,在IP核的设计、物理综合、封装等各个层次都能检测到。

(5)鲁棒性高。水印在嵌入之后很难被各种常规处理与攻击移除或者破坏。

(6)透明性高。水印不影响IP核复用时系统设计与电路设计功能,不易被用户发现。

当然,要完全满足以上6个方面要求的IP核水印技术几乎不存在,我们只能根据IP核的具体类型和使用场景做一些取舍。

目前针对IP核数字水印的研究主要分为以下几类:

(1)基于约束的数字水印;

(2)基于附加的数字水印;

(3)基于模块的数字水印;

(4)基于功率的数字水印。

其中,基于约束和基于模块的数字水印是目前研究的热点。

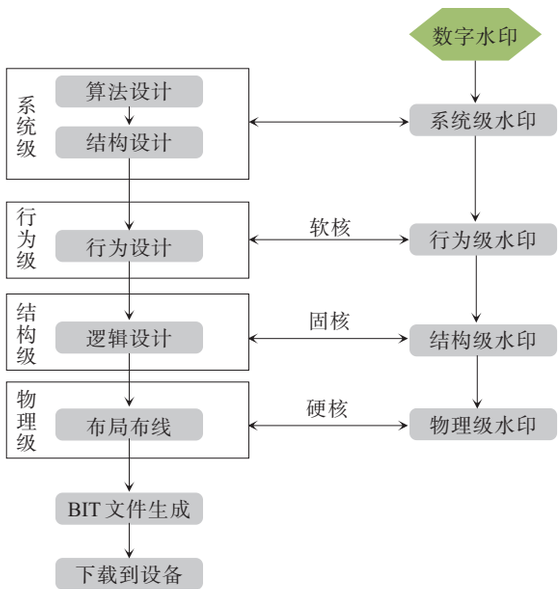

图2 IP核数字水印技术框架图

Fig.2 IP core digital watermarking framework

3.1 基于约束的数字水印

基于约束的IP核水印方法原理是基于集成电路中广泛存在的约束满足问题(SAT)。这一类的IP水印方法可以在算法级、行为级、逻辑综合和物理设计以及FPGA的设计中被有效的证明[19]。通常的策略是把作者的签名映射到一组约束,给定一个伪随机数发生器和特定类型的约束,每个约束都是独立的。假设作者的签名是文字或者图像信息,用*hash*函数(一种单向处理函数)把这些信息转化为密码随机位流,用这个*hash*函数作为流密码的种子。选择约束的不同类型和排列可以得到不同的形式的水印设计实例。这就是一个特定的水印算法例化。IP设计者可以在多个设计阶段加入水印,在相对应的层级检测出这些水印。由于现在IP核以物理层级的硬核交付较多,所以相应的IP核约束水印研究也比较多。

为了证明某个阶段的IP核带有其水印,IP设计者必须指出其水印约束。通过验证水印约束,确定它们中间有多少能够得到满足,根据一定的算法或者公式计算概率*Pc*(满足一致性的约束可能性)。当*Pc*足够小时就能证明设计者签名的存在性。

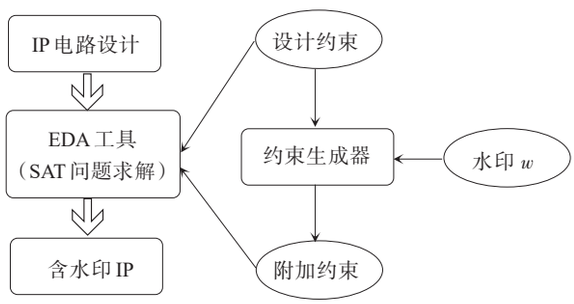

图3 基于约束IP核水印

Fig. 3 IP watermark based on constraint

3.2 基于附加(Additive)的数字水印

与约束水印一样,附加数字水印嵌入设计者的签名信息到IP核中但并不修改IP核的功能,只是利用电路中的一些未用的特殊结构(例如查找表与端口)。这种方法的不足之处是由于水印不是功能电路的一部分,IP核水印很容易被移除,不影响电路功能。现在的研究方向是令水印信息伪装起来像是电路功能的一部分。附加水印在FPGA的设计中应用的比较多。

3.3 基于模块的数字水印

基于模块的数字水印主要是针对IP软核的设计。从电路安全性的角度来看,以GDSII为交付对象的IP硬核是最安全的,因为非常难以做反向工程或者修改。IP软核就具有更高的灵活性,但是也更容易被修改和盗用。随着IP软核复用的增加,其安全性的关注与研究也逐渐增加。硬核的一些水印嵌

入方法例如布局布线与时序约束的水印对IP软核也不适用。在此基础上,有研究者提出了基于模块的数字水印方法,主要分为模块复制与模块分割2种办法。

数字电路的HDL代码中基本的功能模块被其他模块在同一或者更高层级多次调用,这些不断的实例化的模块可以用另外的代码描述相同的功能。基于模块复制的方法基本思想正是来源于此。例如,在一个包含不定态的模块中,这些不定态可以被赋成不同的值,从而产生了多种模块。

3.4 基于功率的水印

这种方法的主要原理就是利用FPGA中的电源管脚进行水印嵌入与检测,由Ziner等[20]首次提出。在FPGA单元中,功耗有静态与动态2种模式。静态模式来源于CMOS传输器的电流泄露,动态模式来源于传输器直接的转换,其中电容是持续加载,短路电流是与时钟边沿同时出现。相应的,FPGA核的电源电压也会出现短时的波动。由于这个原因,通过电源管脚的电源电压与时间的曲线图可以观测出时钟频率。通过FPGA结构中添加的移位寄存器之类的电源分流组件实现水印的嵌入。这些移位寄存器可以由组合逻辑或者不同于FPGA工作频率的时序逻辑组成。针对FPGA电源管脚的频谱分析显示存在2个峰值,一个出现在工作频率,另一个出现在添加组件的频率。其中,组合逻辑的时钟振动会令水印频率的检测变得困难。

基于功率水印的缺点之一是设计代价比较大。文献[21]指出基于功率分析的数字水印很容易遭受攻击,例如通过反向工程或者移除移位寄存器来移除水印。另一个问题是信噪比(SNR)的存在导致攻击者可以通过插入FPGA额外的组件来降低信噪比,从而使功率水印难以检测出来。

Potkonjak团队于1997年开发了第一批硬件水印和指纹识别方法,并于1998年初报道了DSP [22]和FPGA [23]设计。从那时起,数字水印已应用于IC设计的几乎每个阶段,以保护各种设计IP从物理版图到Verilog代码,并以组合电路和时序逻辑以及抽象计算模型(例如有限状态)的形式提供保护机器和图形模型。早期的大部分工作都包含在2003年出版的书[24]中,最新的工作可以在2016年出版的一本书章节中找到[25]。核心是在各个设计阶段添加额外的约束,以嵌入IP所有者(称为水印)和合法IP用户(称为指纹)的签名。这些约束不会影响IP的功能,但会导致IP实施中的“不必”要和“随机”结构和属性。这些结构和属性的存在将用于“概率”地建立IP所有权或识别IP用户。创建、嵌入和提取这些附加约束的特定方法是特定于设计的。

4 硬件计量

基于复用的设计方法和内部芯片制造设施的昂贵成本已使大多数设计公司变为无晶圆厂,他们不得不将设计外包给第三方的代工厂。这样代工厂就可以访问芯片的详细信息,并且可以在未经设计公司授权的情况下进行过度制造。因此,不可信的代工厂可能成为IP过度制造的侵权者。数字水印无法解决此问题,因为多余的芯片带有设计公司的真实水印。尽管指纹可以识别每个芯片,但是过度制造的芯片只会使拥有相同指纹的用户成为过度制造芯片的来源。因此,需要新的方法来防御这种IP侵权,解决方案是IC计量,这是一种有效的协议,可使设计公司对其IC进行制造后控制。

IC计量的基本概念是在每个IC上嵌入一个唯一的签名,并确保签名在设计公司而不是代工厂的控制之下。已经提出了许多不同类型的签名并将其用于硬件计量,可以根据各种标准对其进行分类[26]。

被动计量的签名只能用于芯片识别,而主动计量的签名也可以启用、禁用或控制芯片。根据这种控制是否是设计的一部分,主动计量可进一步分为内部控制和外部控制。内部计量不需要外部组件的帮助或设计的修改,而外部计量方法则需要。根据签名是否与芯片功能交互,可采用非功能计量和功能计量。最后,根据签名是否可以复制,可进一步划分为可复制和不可克隆的签名。

5 硬件混淆

尽管上述数字指纹、数字水印和硬件计量方法可以阻止IP盗版,但它们并不能积极防止IP盗版的发生或使IP盗版更加困难。通常大多数IP盗版都是

从反向工程开始的,通过设计混淆可增加反向工程的复杂性。本节重点介绍2种最近开发的硬件混淆方法:逻辑锁定[27]和IC伪装[28]。

这2种方法的共同特点是将修改电路的设计和制造,以使反向工程攻击者无法获得有效的门级网表进行IP盗版。在逻辑锁定中,将诸如XOR之类的附加门插入非关键节点中。添加到此类门的输入是称为密钥的控制信号。仅当提供正确的密钥值时,电路才能正常工作。假定攻击者将无法访问存储在安全存储器中的密钥值。有了这样的密钥,IP所有者就可以在公共密钥基础结构(PKI)的支持下控制芯片[27]从这个意义上讲,这种方法也称为逻辑加密。这将有效地防护恶意IP用户和不可信的代工厂。

另一方面,电路伪装是基于以下事实:反向工程技术通常比最新设计技术落后2至3代。例如,反向工程工具将无法检测某些相邻金属层之间的虚拟和真实接触。通过利用这些限制,可以以某种方式制造电路,以使某些具有不同功能的单元(例如NAND,NOR和XOR)看起来与反向工程攻击者相同。为了提取IP的真正功能,攻击者需要付出额外的努力[28],其他IC伪装方法使用始终导通和始终截止的MOS晶体管,或者通过存储在SRAM中的信息来配置伪装的单元,或者利用新兴器件的特殊特性。

硬件混淆是IP保护中十分活跃的主题之一,提出了许多潜在的攻击来伪装电路和相应的对策。逻辑加密和IC伪装都可以用来防御反向工程攻击,只有逻辑加密可以帮助抵御不可靠的晶圆代工厂,因为IP所有者可以控制密钥。另一方面,IC伪装在这种情况下可能没有用,除非采用硅后工艺可配置伪装单元,否则必须将所有伪装单元的详细信息发布给代工厂以进行正确的制造。

6 结 论

IP保护已成为基于复用的设计方法的关键支持技术之一。多年来,IP保护机理的研究和开发取得了重大进展。本文详细讨论IP保护的主要方法,包括加密与许可证机制、数字指纹、数字水印、IC计量、硬件混淆等。对于IP所有者而言,不仅面临竞争对手的威胁,而且还面临IP用户和代工厂的潜在知识产权侵权。为了获得全面的保护,必须尽可能采取诸如版权和专利等具有威慑力的法律手段,这仍然是弥补因知识产权盗版而损失的唯一合法途径。为了验证IP侵权,出现了各种IP保护方法,数字水印可确定IP的作者身份;数字指纹可以追踪IP和IP侵权者;硬件计量可防止代工厂过度制造芯片;电路混淆可增加反向工程的难度;分开制造可避免将设计信息泄漏给不可信的代工厂。在采用各种IP保护方法之前,应考虑针对特定应用的设计约束和IP侵权模型。总而言之,IP保护是一项系统工程问题,需要采用整体方法来解决。

尽管如此,我们还是应该意识到IP保护方法的局限性。数字水印与数字指纹等IP保护方法毕竟是一种被动的方法,无法第一时间阻止反向工程与IP盗用,可以借鉴目前IC版权主动保护功能锁定与扫描锁定的思想,开发出针对IP核的保护方法。另外基于物理不可克隆函数(PUF)等一些芯片ID的思路也可以借鉴到IP保护。

参考文献

[1] Intellectual Property Protection Development Working Group. intellectual property protection: schemes, alternatives and discussion[R]. VSI Alliance, White Paper, Version 1.1, August 2001.

[2] WANG H, MARKOV I L, LACH J, et al. Watermarking techniques for intellectual property protection[C]// Design Automation Conference. IEEE, 1998: 776-781.

[3] ABDEL-HAMID A T, TAHAR S. Fragile IP watermarking techniques[C]// Proceedings of the NASA/ESA conference on Adaptive Hardware and systems. NASA, 2008: 513-519.

[4] XU W, ZHU Y. A digital copyright protection scheme for soft-IP core based on FSMs[C]// International Conference on Consumer Electronics Communications and Networks (CECNet). IEEE, 2011: 3823 - 3826.

[5] YUAN L, PARI P R, GANG Q. Soft IP protection: watermarking HDL codes[J]. Lecture Notes in Computer Science, 2004, 3200: 224-238.

[6] CASTILLO E, PARRILLA L, GARCIA A, et al. IPP Watermarking technique for ip core protection on FPL devices[C]// International Conference on Field Programmable Logic and Applications(FPL). IEEE, 2006: 1-6.

[7] LACH J, MANGIONE-SMITH W H, POTKONJAK M. Fingerprinting techniques for field- programmable gate array intellectual property protection[J]. IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems, 2006, 20(10): 1253-1261.

[8] QU G, YUAN L. Secure hardware IPs by digital watermark [M]// Introduction to Hardware Security and Trust, Springer, 2012: 123-141.

[9] KIROVSKI D, LIU D, WONG J, et al. Forensic engineering techniques for VLSI CAD tools[C]// 37th Proceedings of Design Automation Conference. IEEE, 2000: 580 - 586.

[10] POTKONJAK M, QU G. Analysis of watermarking techniques for graph coloring problem[C]// IEEE/ ACM International Conference on Computer- Aided Design (ICCAD). IEEE, 1998: 190 - 193.

[11] WOLFE G, WANG H, MARKOV I L, et al. Robust IP watermarking methodologies for physical design[C]// Proceedings of Design Automation Conference. IEEE, 1998: 782--787.

[12] FAN Y C, SHEN J H. DFT-Based SoC/VLSI IP protection and digital rights management platform[J]. IEEE Transactions on Instrumentation & Measurement, 2009, 58(6): 2026-2033.

[13] CHANG C H, CUI A. Synthesis- for- testability watermarking for field authentication of VLSI intellectual property[J]. Circuits & Systems I Regular Papers IEEE Transactions on, 2010, 57(7): 1618-1630.

[14] CUI A, CHANG C H, TAHAR S, et al. A robust FSM watermarking scheme for IP protection of sequential circuit design[J]. IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems, 2011, 30(5): 678-690.

[15] GÖREN S, UGURDAG H F, YILDIZ A, et al. FPGA design security with time division multiplexed PUFs[C]// International Conference on High Performance Computing and Simulation (HPCS). IEEE, 2010: 608-614.

[16] FIN A, FUMMI F. A web-CAD methodology for IP-core analysis and simulation[C]// 37th Proceedings of Design Automation Conference, IEEE, 2000: 597-600.

[17] HINES K, BORRIELLO G. A geographically distributed framework for embedded system design and validation [C]// Proceedings of Design Automation Conference, IEEE, 1998: 140-145.

[18] CALDWELL A E. et al. Effective iterative techniques for fingerprinting design IP[J]. IEEE Transactions on Computer- Aided Design of Integrated Circuits and Systems, 1999, 23(2): 208 - 215.

[19] KAHNG A B, LACH J, MANGIONESMITH W H, et al. Constraint- based watermarking techniques for design IP protection[J]. IEEE Transactions on Computer -Aided Design of Integrated Circuits and Systems, 2001, 20 (10): 1236-1252.

[20] ZIENER D, TEICH J, Evaluation of watermarking methods for FPGA- based IP- cores[R]. Technical report, University of Erlangen-Nuremberg, 2005: 1-18.

[21] BECKER G, KASPER M, MORADI A, PAAR C, Side-channel based watermarks for integrated circuits[C]// IEEE International Symposium on Hardware- Oriented Security and Trust (HOST). IEEE, 2010: 30-35.

[22] HONG I, POTKONJAK M. Techniques for intellectual property protection of DSP designs[C]// International Conference on Acoustics, Speech and Signal (ICASSP). IEEE, 1998: 3133-3136.

[23] LACH J, MANGIONE-SMITH W H, POTKONJAK M. Fingerprinting digital circuits on programmable hardware [C]// International Workshop on Information Hiding. Springer, 1998: 16-31.

[24] QU G, POTKONJAK M. Intellectual property protection in VLSI design: Theory and Practice[M]. Boston: Kluwer Academic Publishers, 2003.

[25] CHANG C H, POTKONJAK M, ZHANG L. Hardware IP watermarking and fingerprinting[M]// Secure System Design and Trustable Computing. Springer, 2016: 329-368.

[26] KOUSHANFAR F. Hardware metering: a survey[M] // Introduction to Hardware Security and Trust. Springer, 2012: 103-122.

[27] ROY J A, KOUSHANFAR F, MARKOV I L. EPIC: ending piracy of integrated circuits[C]// Design Automation and Test in Europe. IEEE, 2008: 1069-1074.

[28] RAJENDRAN J, SAM M, SINANOGLU O, KARRI R. Security analysis of integrated circuit camouflaging[C]// ACM Conference on Computer Communications and Security. ACM, 2013: 709-720.