第 23 卷第 10 期　　半　导　体　学　报　　Vol. 23, No. 10
2002 年 10 月　　CHINESE JOURNAL OF SEMICONDUCTORS　　Oct., 2002

基于核的信息安全处理芯片可测性设计*

陆思安　何剑春　严晓浪　何乐年

(浙江大学超大规模集成电路设计研究所, 杭州　310027)

摘要: 从可测性设计角度讨论了信息安全处理芯片的芯片级测试控制器的设计以及相应核的可测性设计. 综合结果显示, 所设计的芯片级测试控制器所占用的面积代价非常小.

关键词: 可测性设计; 基于核设计; 测试总线; 芯片测试控制器

EEACC: 1265B; 2570F; 5230

中图分类号: TN702　　**文献标识码**: A　　**文章编号**: 0253-4177(2002)10-1112-04

1　引言

随着半导体工艺技术的进一步发展, 芯片的设计规模变得越来越大, 尤其在进入深亚微米工艺后, 芯片的设计已达到了几百万门规模, 系统芯片(SOC)正逐渐变成现实. 然而采用过去的时序驱动设计(timing-driving design)来一次性完成这样大规模的电路设计是不现实的, 于是人们采用基于核设计方法来降低设计的复杂性. 基于核设计就是将一个复杂的设计划分成若干个核分别实现, 然后再将它们集成为一个具有特定功能的芯片的过程. 基于核设计主要由两个部分组成, 即核实现和核集成. 当前不是所有的核都需要自己设计, 我们可以直接使用来自第三方的 IP 核, 进行设计重用(design reuse); 而核的集成就是将自己设计的核和重用的 IP 核集成形成芯片的过程. 但芯片集成决不是一些核的简单堆砌, 在集成过程中不仅要考虑它们的功能, 更要使它们融入到芯片中, 其中一个非常复杂的问题就是如何将具有不同测试结构的核集成在一起形成芯片级测试结构.

当前, 芯片级测试结构普遍基于测试总线(test bus)[1]利用芯片级测试控制器实现对片上所有核的测试控制. 文献[2]详细讨论了与测试重用(test reuse)相关的各种问题; 文献[3]则提出了一个与 IEEE P1500 标准相兼容核的测试存取机制(test access mechanism) CAS-BUS; 文献[4]则提出了一种层次化的测试控制结构, 该结构既兼容符合 IEEE P1500 标准的核, 也兼容符合 IEEE 1149.1 标准的核; 文献[5]则重点讨论了核测试环的设计以实现测试重用. 这些文献都侧重于实现测试重用的标准化问题, 因而测试控制器非常复杂. 对于一个由几十个 IP 核组成的非常复杂的芯片而言, 这样的测试代价是合理的; 然而对于一个相对简单且大部分核都由自己设计的芯片而言, 采用这样的复杂测试控制器就显得不够合理. 本文提出的测试控制器设计方案面向一种信息安全处理芯片, 该信息安全处理芯片由六个核组成, 即一个微控制器(MCU), 直接采用 ARM 公司 IP 核, 两个加密核, 一个 PCI 接口核, 一个 PC Card 接口核, 一个片上嵌入式存储器内建自测试核 MBIST(memory built-in self testing). 除 MCU 采用 IP 核外, 其它各核均由自己设计, 所以我们可以在核的设计过程中就考虑芯片测试控制器的设计问题, 从而大大简化测试控制器的设计.

2　测试总线

IP 核的可测性设计通常采用扫描设计. 这是因为扫描设计方法不仅很好地解决了电路中时序单元的测试, 而且扫描设计生成的扫描链为电路中的组合逻辑部分提供了激励加载通路和响应观测通路, 这使得集成电路的测试向量生成过程实现自动化,

* 国家高技术研究发展计划资助项目(编号: 2001AA140105)

2002-01-21 收到, 2002-04-09 定稿

大大缩短了测试向量的生成时间, 从而缩短产品的上市时间.

内建自测试是可测性设计的另一种重要的方法. 这种方法的基本思想是由电路自己生成测试向量, 而不是要求外部施加测试向量, 它依靠自身逻辑来判断所得到的测试结果是否是正确. 由于需要片上产生测试向量, 而对于随机逻辑而言, 要在片上实现测试向量生成则是个非常复杂的问题, 因此一般而言, 内建自测试 BIST 用在存储器测试上, BIST 虽然可以测试存储器, 但它无法解决 BIST 电路自身的测性, BIST 控制电路一般作为一个独立的核进行扫描综合实现测试. 因此, 在一个芯片中绝大部分都是采用扫描的可测性设计, 芯片的测试结构就是要为每一个 IP 核提供适当扫描测试接口.

从原理上说, 芯片内所有的扫描寄存器都可连在一起形成一条扫描链实现测试. 但在实际的设计中, 扫描链一般不宜过长, 因为扫描链越长, 数据从扫描链的一端移到另一端需要的时间就越多, 这样芯片的测试费用就越高, 从而增加芯片成本. 因此对于一个较大的基于扫描设计的 IP 核, 往往将它划分成多条扫描链, 从而加快测试速度, 而一个芯片又是由若干个 IP 核组成, 如果每个 IP 核扫描链的扫描数据输入输出都连接到芯片的外部输入输出引脚上, 则所需要的引脚数目就太多, 从而增加芯片封装费用, 进而增加芯片成本. 通常在芯片中采用测试总线结构, 如图 1 所示. 图中的芯片由八个核组成, MCU 是一种可编程 CPU 核, 它在芯片中处于核心地位; core1、core2 以及 core7 均为具有特殊功能的 IP 核; sdi 为扫描数据输入, sdo 为扫描数据输出, 每个核的扫描链一般都不止一条, 这些扫描链组织在一起就构成了所谓的测试总线.

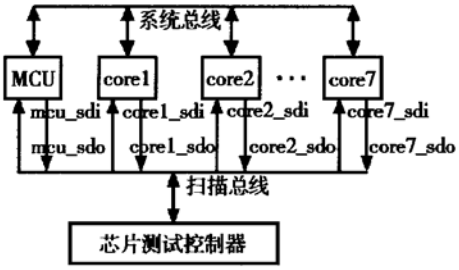

图 1　测试总线原理图

Fig. 1　Diagram of scan bus

测试总线的宽度等于各 IP 核扫描链数最大值的两倍. 取两倍是因为一条扫描链需要两个扫描数据端口, 即一个扫描数据输入, 一个扫描数据输出. 假定 core1 有 5 条扫描链, core1 扫描数据端口数是 10; core2 有 6 条扫描链, 则 core2 的扫描数据端口数是 12, 这样测试总线的宽度就应该取 12.

核的扫描链数目是不定的, 有的多有的少. 如果不管扫描链的数目多少, 所有核都进行单独测试, 则对于扫描链数目较少的核来说就是资源浪费. 这时可以将几个扫描链数目较少的核组合在一起共用一组测试模式控制信号, 同时进行测试.

3　芯片级测试控制器设计

从测试角度看, 芯片至少有两种工作模式: 正常的功能模式和芯片中单个核测试模式. 一般芯片中的核不止一个, 当某个核进行测试时, 其它核最好处于静止状态. 这样控制一个核的测试应该有两个测试控制信号, 即扫描模式信号 sm 和测试复位信号 trst, 如图 2 所示. 这两个信号均是低电平有效, 它们都是由芯片测试控制器产生.

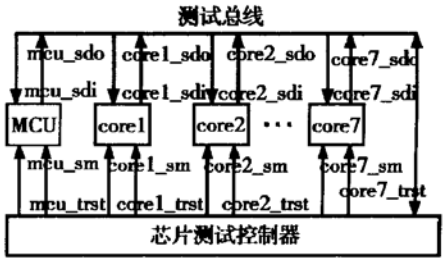

图 2　芯片测试控制器原理图

Fig. 2　Diagram of chip test controller

当 sm= 1, trst= 1 时, 核处于正常功能模式; 当 sm= 0, trst= 1 时, 核处于扫描测试; 当 sm= 1, trst= 0 时, 核处于静止状态. 一个典型的芯片测试控制器设计如图 3 所示. test 是一个总控信号, 当 test= 1 时, 所有的扫描模式信号和测试复位信号均为 1, 这样芯片就处于正常功能模式; 而要想芯片进入测试状态, 首先将 test 置 0, 然后再分别控制相应测试模式信号 tm0、tm1、tm2 选择希望测试的核.

系统芯片是将一些复杂的功能单元集成到一个单独的芯片上, 即它在一个芯片上就实现系统的所有功能, 因此 SOC 的设计规模一般都很大, 芯片内核的数目可能达十几个, 这样扫描模式信号也就需要十几个. 如此之多的扫描模式信号就不宜直接连接到芯片的封装引脚上, 简单的解决方法是采用译

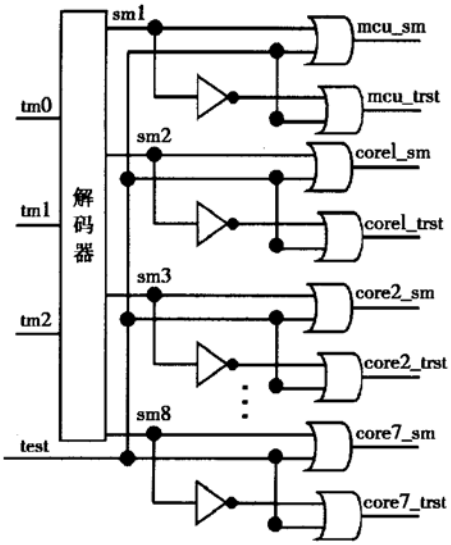

图 3 芯片测试控制器的设计

Fig. 3 Design of chip test controller

码器, 这样就可以减少封装引脚的数目. 图 3 中芯片有 8 个核, 采用一个 3-8 译码器, 这样测试模式控制信号减少为 4 个.

基于同样目的, 测试总线也不是直接连接到芯片的封装引脚上, 而是与功能引脚共享, 这样在测试控制器中必须在每个输入输出引脚上增加一个多路器. 不过引脚共享时注意避免与双向功能端口共享, 应是扫描输入输出端口与功能输入输出端口共享.

4 采用测试总线结构的核在设计上的一些特殊考虑

4.1 复位信号设计

前面已经说过, 芯片中当某个核进行测试时, 其它核应该处于静止状态. 比如当 core1 进行测试时, core2、core3 最好处于静止状态. 要达到这个目的, 最简单的方法就是直接控制复位信号, 使不进行测试的核处于复位状态, 如图 4 所示. 测试复位信号 trst 是低电平有效, 芯片复位信号 rst 高电平有效, 生成的核复位信号 core_rst 也是高电平有效. 其真值表如表 1 所示.

值得注意的是该电路引入了核扫描模式信号 core_sm, 这是为了保证核在扫描测试时(即 core_sm= 0) 外部复位信号 rst 不会干扰核的扫描测试.

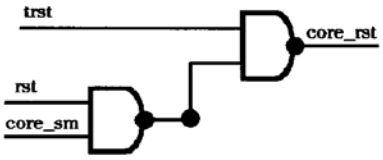

图 4 复位信号设计

Fig. 4 Design of reset signal

表 1 复位电路的真值表

Table 1 True value table of reset circuits

工作模式		rst	core_sm	trst	core_rst
功能模式	功能操作	0	1	1	0
	复位操作	1	1	1	1
测试模式		x	0	1	0
复位模式		x	1	0	1

4.2 扫描允许信号设计

在一个芯片中, 芯片扫描允许信号 se 是一个全局信号. 在扫描测试过程中 se 是变化的, 因为扫描测试过程中存在两种操作, 即扫描移位操作和测试向量施加及测试响应抓取操作. 当信号 se= 1 时, 进行扫描移位操作; 当 se= 0 时, 进行测试向量施加及测试响应抓取操作. 因此, 如果不对 se 信号进行约束的话, 当核处于非测试状态时, 它仍可能引起核的某些逻辑动作, 从而增加测试功耗, 甚至引起电路某些误动作. 故我们用核的扫描模式信号对其进行门控, 如图 5 所示. 这样在 core_sm= 1 时, core_se 始终为 1.

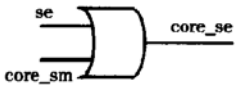

图 5 扫描允许信号设计

Fig. 5 Design of scan enable signal

4.3 扫描输出端口设计

由于采用测试总线技术, 在某一特定时刻, 只有处于测试状态下的核扫描数据输出 sdo 端口驱动总线, 而不处于测试状态下的所有核的扫描数据输出 sdo 端口处于高阻状态, 如图 6 所示. 其中输出允许信号采用核扫描允许信号 core_se.

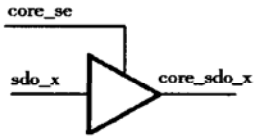

图 6 扫描数据输出端口设计

Fig. 6 Design of scan data output ports

5　实验结果及结论

依据本文第三部分所述的原理, 我们利用 Verilog 语言编写了测试控制器并用 VCS 进行了验证, 然后采用 SYNOPSYS 公司的 DC(design compiler) 进行综合, 综合结果显示该测试控制器所占用的面积仅为 43 等效门(没有考虑布线代价). 文献[1] 中给出一个设计是: 1 个 CPU 、1 个 ROM 和 3 个其它核, 该设计测试代价为 500 个门; 而文献[3] 在测试总线 N 为 6, 每个 CAS 的开关线数目 $P=1$ 时, 每个核测试代价为 33, 六个核就为 198. 如果各个核扫描链数目增加, 则 P 可能增加. 当 $P=2$ 时, 每个核的测试代价为 134 个门; 当 $P=3$ 时, 单个核测试代价为 280 个门. 从这里可以看出, 本文提出的测试控制器的面积代价相当小. 采用同样原理, 我们还实现了片上达到 16 个核时测试控制器, 综合结果为 109 等效门; 而当片上核为 32 个时, 测试控制器的面积也仅为 149 等效门.

集成电路设计是一个非常复杂的过程, 在设计过程中要考虑到方方面面的问题, 它实际上是针对不同设计目标不断进行权衡的过程. 而在不同情况下芯片测试控制器可以有不同设计. 本文针对芯片设计规模不是很复杂, 芯片中的大部分核均是自己设计这种情况提出了一种芯片测试控制器, 综合结果显示该测试控制器的实现与其它芯片测试控制器相比较要简单得多.

参考文献

[1] Ono T, Wakui K, Hikima H, et al. Integrated and automated design-for-testability implementation for cell-based ICs. Proceedings of Test Symposium, 1997: 122

[2] Varma P, Bhatia B. A structured test re-use methodology for core-based system chips. Proceedings of Test Conference, 1998: 294

[3] Benabdenebi M, Maroufi W, Marzouki M. CAS-BUS: a scalable and reconfigurable test access mechanism for systems on a chip. Proceedings of Design, Automation and Test in Europe Conference and Exhibition, 2000: 141

[4] Lee Kuen-Jong, Huang Cheng-I. A hierarchical test control architecture for core based design. Proceedings of the Ninth Asian Test Symposium, 2000: 248

[5] Marinissen E J, Arendsen R, Bos G, et al. A structured and scalable mechanism for test access to embedded reusable cores. Proceedings of Test Conference, 1998: 284

Core-Based Security Chip Design for Test*

Lu Sian, He Jianchun, Yan Xiaolang and He Lenian

(Institute of VLSI Design, Zhejiang University, Hangzhou 310027, China)

Abstract: The design of chip test controller of a security chip and design for test of corresponding cores are discussed in detail. The results of the synthesis show that area overhead of the chip test controller is quite small.

Key words: design for test; core-based design; scan bus; chip test controller

EEACC: 1265B; 2570F; 5230

Article ID: 0253-4177(2002)10-1112-04

* Project supported by National High Technology Research and Devehopment Programm of China(Grant No. 2001AA140105)

Received 21 January 2002, revised manuscript received 9 April 2002