

# 一种关于信息安全专用集成电路的测试验证系统

曹维安, 白国强

(清华大学 微电子学研究所, 北京 100084)

**摘 要:** 针对信息安全专用集成电路输入输出数据宽度大, 无法做到测试全覆盖的特点, 本文提出并实现了一种专门测试此类电路功能、性能的测试验证系统。该系统基于 PC 机, 采用 PCI 软件和 FPGA 等硬件配合的方式, 能够满足待测芯片对大批量数据高速传输需求。通过对一款椭圆曲线密码专用集成电路的测试, 证明该系统具有成本低, 便于调试、演示, 代码通用性强, 系统复制、移植方便等特点。该系统对解决信息安全专用集成电路的测试问题具有重要参考价值。

**关键词:** 信息安全专用集成电路; 测试系统; PCI; FPGA; 椭圆曲线密码

**中图分类号:** TN918

**文献标识码:** A

**文章编号:** 1000-7180(2013)01-0148-05

## A Testing System for Application Specific Integrated Circuit of Information Security

CAO Wei-an, BAI Guo-qiang

(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

**Abstract:** This paper presents a test and verification system which specially tests the function and property of information security ASIC, for that input and output data of such circuits often have large width and the test can not cover all cases. The system based on PC is implemented by cooperation of PCI software, FPGA and other hardware in order to meet tested chip's demand of high-speed transmission of large amounts of data. The test of an elliptic curve cryptography ASIC proves that the system has low cost, universal code, easy debugging, easy presenting and easy transplanting features. It also has important value to solve the problem of information security ASIC testing.

**Key words:** information security ASIC; test system; PCI; FPGA; elliptic curve cryptograph (ECC)

### 1 引言

随着微电子技术的发展和应用需求的推动, 越来越多信息安全解决方案中的密码算法通过专用集成电路方式实现, 信息安全专用集成电路的设计、制造、测试和应用开发已成为信息技术领域的研究热点。能够实现一个或多个密码算法的信息安全专用集成电路, 其特点是数据的输入和输出宽度很大, 对该类电路的测试一般无法做到全覆盖。例如, 关于分组密码算法 AES 的专用集成电路, 其输入和输出的数据宽度都是 128 比特, 全部不同的输入向量有  $2^{128}$  个, 不可能把这些全部不同的向量输入电路以测

试其运算功能的正确。为此, 关于信息安全专用集成电路的测试, 都采用了随机覆盖的方法进行测试。为提高测试的可靠性, 在有限的时间内尽力以更多的测试向量输入电路对其进行测试是一种正确的策略。因此, 构建高速测试系统以实现对信息安全专用芯片的测试, 尽力提高其可靠性是十分重要的。

本文针对信息安全专用集成电路的测试和验证, 提出一种软、硬件结合的测试系统, 并通过对一款椭圆曲线密码芯片的测试, 证明该系统具有成本低, 便于调试、演示, 代码通用性强, 系统复制、移植方便等特点, 能够很好地满足实际中对信息安全专用集成电路的测试。

**收稿日期:** 2012-05-04; **修回日期:** 2012-06-01

**基金项目:** 国家自然科学基金项目(60576027, 61073169); 国家“八六三”计划项目(2006AA01Z415)

## 2 硬件组成与系统架构

该系统由 PC 软件主导,以 PCI9054 芯片为桥梁,SRAM 为缓存,FPGA 及相关硬件协调配合来实现.系统硬件架构如图 1 所示.除 PC 机和待测芯片外,测试系统主板主要由一块 FPGA 芯片、一块 PCI9054 芯片<sup>[1]</sup>、一块 EEPROM 芯片、一块 SRAM 芯片<sup>[2]</sup>、两块 EPROM 芯片和一块随机数生成 RNG 芯片组成.该 PCB 板与 PC 机通过 PCI 插槽相连.

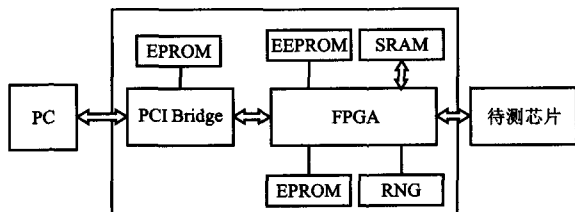


图 1 系统架构图

另外设计一转接子板,连接 FPGA 和待测芯片.子板与 PCB 板之间通过 2mm 通用接口连接.子板为待测芯片提供电源和插座,电源芯片选用 LM1117-1.8 型稳压芯片<sup>[3]</sup>.为了能够利用演示系统对同类型的多枚芯片进行演示,子板上使用了 IC 测试插座<sup>[4]</sup>,而不是直接将待测芯片焊接在转接子板上.

系统的数据流如图 2 所示. PC 主机端软件通过 PCI9054 芯片发送数据,经 FPGA 接口逻辑处理,写入 SRAM 缓存 rd\_buf;FPGA 适时将 rd\_buf 缓存中数据读出,通过与待测芯片接口逻辑写入待测芯片内部存储器;FPGA 适时将待测芯片计算结果读出并写入 SRAM 缓存 wt\_buf;主机端软件适时将 wt\_buf 存储的计算结果通过 PCI 芯片读回 PC 机并以文本形式保存.显然 PCI9054 芯片应该工作在从模式,这样才能保证 PC 对自己的读写操作.在这个系统中,数据传输的最大瓶颈在于 PCI 接口部分,而 PCI9054 芯片仅以单周期读写的传输方式就能够提供超过 10Mbps 的传输速度.

上述数据流过程中,因为涉及到数据的大量传输,SRAM 每块缓存能否有效、有序使用成为一个重要问题.提出同步标记比特的概念:FPGA 内部设两个寄存器组,分别同步标记 rd\_buf 和 wt\_buf (以一组数据的长度为单位划分).PC 端软件和 FPGA 共同维护 synch\_bit\_up、synch\_bit\_down 这两个寄存器组,PC 端控制 h\_p、s\_p 指针,FPGA 端控制 h\_ptr、s\_ptr 指针.

同步 bit 控制缓存示意图如图 3 所示. PC 每次

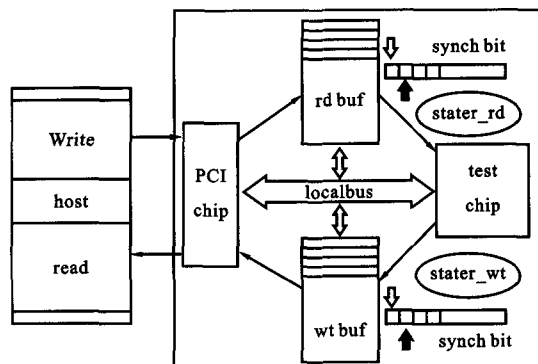


图 2 数据流程图

发送数据前,首先查看 h\_p 所指缓存是否为空,若为空则发送一组数据到 rd\_buf 相应位置,然后将 synch\_bit\_up 相应标记位置为有效.同理,PC 每次读取数据前,需查看 s\_p 所指缓存是否有效,若有效则从 wt\_buf 相应位置读取一组结果数据,然后将 synch\_bit\_down 相应标记位置为空.而 FPGA 则控制 h\_ptr、s\_ptr 两个指针,当 h\_ptr 所指位置有效时,读取相应数据并传给待测芯片,然后将其标记位置为空;当 s\_ptr 所指位置为空时,从待测芯片读取结果数据并写入 wt\_buf 缓存相应位置,再将相应标记位置为有效.每次读写数据之后,相应指针都要向下移一位,达到缓存总长度时则指回初始位置.缓存总长度可在调试中灵活确定.

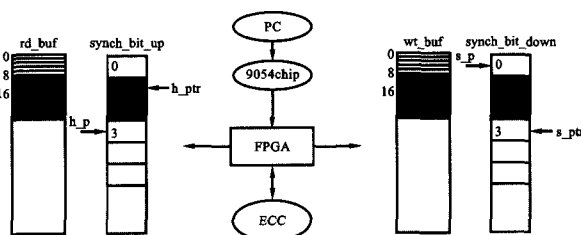


图 3 同步 bit 控制缓存示意图

同步标记位还有一重要作用就是可用来确定读写 SRAM 地址线的具体值.另外,待测芯片内部同样有一块缓存区域,也需要设置一个同步标记数组加以控制.

## 3 PCI 地址划分与译码

PC 端软件与 FPGA 等底层硬件的数据传输,在底层看来,就是 PC 通过 PCI9054 芯片对不同地址读写数据,这需要软件和硬件对不同地址段表示的内容达成一致.

系统中 PCI 地址划分如表 1 所示.将 PCI 地址空间大致分为三部分,包括本地控制寄存器、本地同步标记寄存器和 SRAM 缓存.其中各地址段只表示 PCI 相对地址,即偏移量,加上基址后才是 PCI 实际

地址. 这三部分都可被 PC 端驱动程序通过 PCI9054 桥读写, 本地 FPGA 也可对这三部分进行读写操作.

表 1 PCI 地址划分

| 地址段名称            | 相对地址范围<br>(只列出[23,0]位)     | 说明        |
|------------------|----------------------------|-----------|
| 系统控制寄存器段         | 0x000000 ~ 0x0000ff(256B)  | 用于系统控制    |
| rd_synch_bit     | 0x000100 ~ 0x0004ff(1024B) | 用于同步控制    |
| wt_synch_bit     | 0x000500 ~ 0x0008ff(1024B) | 用于同步控制    |
| rd_buf(SRAM 地址段) | 0x100000 ~ 0x4ffff(8MB)    | SRAM 地址空间 |
| wt_buf(SRAM 地址段) | 0x500000 ~ 0x8ffff(8MB)    | SRAM 地址空间 |

译码操作由 FPGA 根据地址划分情况实现, 通过译码使得每个 PCI 地址都能对应本地单一的存储单元. 以同步 bit 段为例, 即将 PCI 的 0x000100 ~ 0x0004ff(1024B) 地址映射到本地同步寄存器 synch\_bit\_up 的 0—255 地址, 将 PCI 的 0x000500 ~ 0x0008ff(1024B) 地址映射到 synch\_bit\_down 的 0—255 地址.

#### 4 软件和硬件实现

本系统的软件部分主要由应用程序和驱动程序两部分组成, 都在 VC6.0 环境下实现. 软件结构如图 4 所示.

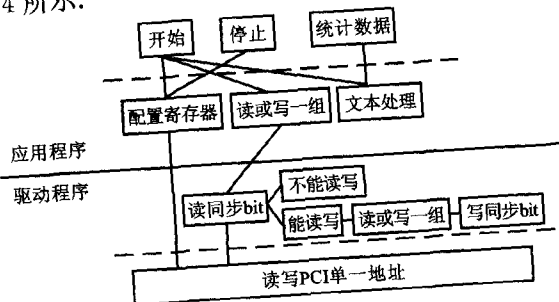


图 4 系统软件结构图

应用程序包括一图形用户界面, 主要负责载入输入数据(txt 形式)、保存结果数据(txt 形式)、发起开始、结束命令、发起初始化命令、发起读或写一组数据的命令、统计速度等. 而响应这些命令、具体实现 PCI 数据读写的任务由驱动程序完成. 应用程序和驱动程序在单组数据长度上需设置一致, 彼此之间需定义指针变量, 通过传递地址来传递数据. 另外, 应用程序可控制 PCI 写、读数据的节奏, 可写一组读一组循环, 也可写多组再读多组循环. 在调试时加入读写间隔时间, 以毫秒为单位. 更重要的, 在测试信息安全专用芯片时, 它可以通过简单编程实现快速覆盖尽可能多的任意一段测试向量. 这里体现了软件在调试时的灵活、高效性.

驱动程序是标准的针对 PCI9054 芯片的驱动程序, 由 inf 文件和 sys 文件两部分组成. inf 文件是文本形式, 包含必要的安装配置信息. sys 文件需在相应驱动程序开发包的配合下编译生成, 除了需要完成相关的配置任务外, 还需响应应用程序的任务命令, 具体实现对某一特定 PCI 地址的读写操作. 之前所规定的软件、硬件之间的各个地址协议其实就是 sys 文件和 FPGA 之间的协议. 根据这些协议, 驱动程序不仅需要 FPGA 内部相关的控制寄存器进行读写配置; 还需要在传输每组数据的同时, 根据同步标记位的方案, 不断维护指向 SRAM 缓存的指针 h\_p, s\_p, 并且将数据读出或写入 SRAM 相应位置以及同步标记数组相应位置.

应用程序、驱动程序、PCI、FPGA、SRAM 组成一条数据传输线路, 该线路以 PC 端软件主导、PCI9054 为媒介、FPGA 配合来实现. 当软件通过 PCI9054 芯片发起传输请求时, FPGA 需响应该请求才能完成该线路的数据传输. 若 FPGA 相关状态机繁忙, 则软件需等待其空闲才能进行传输.

硬件部分主要由 FPGA 采用有限状态机来实现. 结合 PCI 地址划分和译码方案, 实现了 FPGA 与 PCI9054 芯片<sup>[5]</sup>、SRAM 芯片的接口逻辑, 使得软件能够通过 PCI 读写本地 FPGA 或 SRAM 数据. 此外, 还实现了 FPGA 与待测芯片的接口逻辑. 在初始化时, FPGA 不仅要初始化所有 FPGA 内部的相关寄存器, 还要初始化待测芯片, 做相关配置工作. 之后, 进入批量测试阶段. 在此阶段, 除了应用程序、驱动程序、PCI、FPGA、SRAM 数据传输线路外, 还有一个 SRAM、FPGA、待测芯片数据传输线路, 此线路由 FPGA 根据待测芯片需求来主导数据传输过程.

FPGA 根据待测芯片的缓存情况, 可以不断从 SRAM 获取数据填充到待测芯片缓存, 然后根据待测芯片中断信号不断将运算结果读出再写入 SRAM. 同时, FPGA 还需不断维护 h\_ptr, s\_ptr 指针和同步标记数组, 用来确定每次读写 SRAM 的具体地址, 这也使得软硬件能共同有序使用 SRAM. FPGA 主要状态机的关系图如图 5 所示.

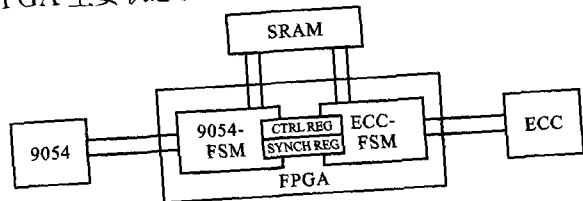


图 5 FPGA 主要状态机关系图

5 ECC 芯片测试

THECC500 芯片<sup>[6]</sup>是一款 ECC 算法专用芯片,芯片支持素数域<sup>[7]</sup>最大位长 384 位,二元域最大位长 383 位的多种椭圆曲线算法,包括点加、倍点、点乘、点是否在曲线上的验证、符合中国椭圆曲线算法标准的签名(以下简称 GB 签名)产生和验证、符合 WAPI 标准的签名(以下简称 WAPI 签名)产生和验证,并可以通过简单的编程实现其他与有限域运算或椭圆曲线运算相关的算法.该芯片由 0.18 微米 CMOS 标准工艺制造,芯片各功能和性能的理论值如表 2、表 3、表 4 所示.

表 2 ECC 芯片点加、倍点、点乘计算平均周期数

| 运算类型       | 周期数                                           |
|------------|-----------------------------------------------|
| 素数域曲线点加    | $5.44n + 49.72$ ( $n$ 为位长,下同)                 |
| 素数域曲线倍点    | $6.44n + 59.72$                               |
| 素数域曲线点乘    | $8.25n^2 + 81.29n + 2X + 33$ ( $X$ 为流水线级数,下同) |
| 特征 2 域曲线点加 | $5n + 33$                                     |
| 特征 2 域曲线倍点 | $5n + 23$                                     |
| 特征 2 域曲线点乘 | $6.67n^2 + 39n + X + 13$                      |

表 3 250 MHz 工作频率下计算一次椭圆曲线点乘所需时间

| 位长 $n$  | 160     | 192    | 256    | 384    |
|---------|---------|--------|--------|--------|
| 素数域     | 0.899ms | 1.28ms | 2.25ms | 4.99ms |
| 特征 2 扩域 | 0.709ms | 1.01ms | 1.79ms | 不支持    |

表 4 233 MHz 工作频率下每秒可以完成的椭圆曲线点乘计算的次数

| 位长 $n$  | 160   | 192  | 256  | 384  |
|---------|-------|------|------|------|
| 素数域     | 8278  | 5814 | 3307 | 1491 |
| 特征 2 扩域 | 10496 | 7368 | 4157 | 不支持  |

利用本文所建立的测试系统,对该芯片的所有功能和计算性能进行了测试.通过简单的 VC 编程,尽可能多的覆盖倍点数,以素数域下 256 位点乘运算为例,用 PCI 时钟 33 MHz 作为 ECC 内部时钟,未使用倍频器,测得 10 秒内总点乘计算数据组数平均为 3711 组,即一秒内计算约 371 组.如果使用倍频器,即 233 MHz 时钟,那么速度将会达到每秒 3000 余组,基本接近表 4 中理论值每秒 3307 组.

单组数据的计算周期数通过 FPGA、chipscope 软件测得(精度为 100 个周期),这里同样可以通过 VC 编程实现尽量多的覆盖倍点数来测得平均值.

素数域 256 位、二元域 233 位点乘运算时钟周期数测试结果如表 5、表 6 所示.素数域平均值为 568700,根据表 2 中理论值, $8.25n^2 + 81.29n$ , $n$  为 256 位长时结果为 57 万,二者一致.二元域平均值为 371363,表 2 中理论值公式可算得约 372000,二者一致.

表 5 实测素数域 256 位点乘周期数

| K 值 | 16 个 A | 32 个 A | 48 个 A | (全 A)  |
|-----|--------|--------|--------|--------|
| 周期数 | 484989 | 531052 | 577173 | 623232 |

表 6 实测二元域 233 位点乘周期数

| K 值 | 1 个 A  | 全 A    | 平均值    |
|-----|--------|--------|--------|
| 周期数 | 279435 | 416749 | 371363 |

完成一组点乘运算的时间与倍数 K 值中 1、0 的分布关系密切,当 K 为  $n$  位数时, $n$  即二倍点运算的次数, $n$  位数中 1 的个数即为点加运算的次数.但根据 CSD 编码,K 若包含连续的 1,那么情况反而简单,所以最复杂的 K 莫过于 256 比特 1、0 交错循环的情况,即 16 进制下全 A.表 5 也验证了这一点,随着 A 的变化,运算周期数基本成等差数列排列.

ECC 芯片素数域下其它功能的运算周期数如表 7 所示.

表 7 素数域其他 ECC 功能平均周期数

| 计算功能 | GB 签名<br>(256 位) | GB 验证<br>(256 位) | WAPI 签名<br>(192 位) | WAPI 验证<br>(192 位) |
|------|------------------|------------------|--------------------|--------------------|
| 周期数  | 572971           | 1143816          | 322872             | 645375             |

ECC 算法中,数字签名运算主要包含一次点乘运算,另外还有整数加、模除等运算.而验证过程主要包含两个点乘运算,另外还有其它辅助运算.选定一组标准椭圆曲线参数、一组固定基点和一固定倍点数,进行 GB 签名运算,测得需 568882 个周期;而用相同的数据进行点乘运算,测得 565518 个周期,二者相差 3364 个周期,此即为签名运算中抛去点乘运算的剩余部分的运算时间,占总周期数的 0.59%.

6 结束语

本文以测试一款 ECC 芯片为例,成功实现了一套软件、硬件结合的信息安全专用集成电路的测试演示系统.该系统可通过简单 VC 编程实现高速覆盖尽可能多的测试向量;PCI 也能够很好满足待测芯片对数据传输速度的需求;同步 bit 控制缓存的方案使得大批量数据在系统中能够高速、有序地传

输;软件方面的架构设计使应用程序和驱动程序层次分工明确,方便灵活调试.该系统具有很好的扩展性和通用性.对于其他信息安全专用集成电路,都可以采用此系统来测试并展示其功能、性能.

与传统大型芯片测试仪相比,本系统基于 PC 机 PCI、VC 软件和 FPGA,开发成本低,系统可复制、可移植性强,测试代码复用性强,且演示效果好.与基于单片机的小型测试系统相比,本系统同样具有更好的测试代码复用性、成本低、可移植性强、演示效果好等特点.

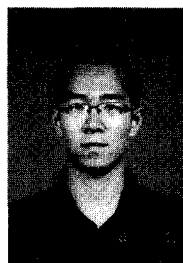
#### 参考文献:

- [1] PLX Technology. Inc. PCI9054 Data Book Version 2.1 [EB/OL]. [2012-05-04]. 2000. <http://www.alldatasheet.com/datasheet-pdf/pdf/210852/PLX/PCI9054.html>.
- [2] SAMSUNG Electronics. K6F3216U6M Data Sheet Version 1.0 [EB/OL]. [2012-05-04]. 2002. <http://www.alldatasheet.com/datasheet-pdf/pdf/111605/SAMSUNG/K6F3216U6M.html>.
- [3] CYSTech Electronics Corp. LM1117L3 Data Sheet [EB/OL]. [2012-05-04]. 2005. <http://www.alldatasheet.com/datasheet-pdf/pdf/141830/CYSTEKEC/LM1117L3>.

html.

- [4] YAMAICHI ELECTRONICS. IC51 Series(Clamshell) Data Sheet[EB/OL]. [2012-05-04]. 2008. [http://www.lm-connector.com/IC测试座\(IC51-QFP-5\).pdf](http://www.lm-connector.com/IC测试座(IC51-QFP-5).pdf).
- [5] 马超,皮亦鸣.基于 PCI9054 的 PCI 接口数据通信系统[J].电子科技大学电子工程学,2008(1):70-73.
- [6] 陈刚.有限域算术和椭圆曲线算术的硬件算法和架构[D].北京:清华大学微电子学研究所,2008.
- [7] Chen G, Bai G, Chen H. A high-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit[J]. IEEE Transactions on Circuits and Systems-2: Express Briefs, 2007, 54(5):412-416.

#### 作者简介:



曹维安 男,硕士研究生.研究方向为信息安全芯片.

(上接第 147 页)

#### 参考文献:

- [1] 贾骥,覃征,卢江,等.圆环射线分解投影轮廓的三维模型检索方法[J].系统仿真学报,2006,18(10):2847-2850.
- [2] Castellani U, Cristani M, Fantoni S, et al. Sparse points matching by combining 3D mesh saliency with statistical descriptors[J]. Computer Graphics Forum, 2008, 27(2):643-652.
- [3] Cao LL, Liu JZ. 3D object retrieval using 2D line drawing and graph-based relevance feedback[C]//Proceedings of the 14th annual ACM international conference on Multimedia[S. L.]:ACM, 2006:105-108.
- [4] Funkhouser T, Min P, Kazhdan M, et al. A search engine for 3D models [J]. ACM Transactions on Graphics, 2003, 22(1):83-105.

- [5] Chen DY, Ouhyoung M. A 3D object retrieval system based on multi-resolution reeb graph[C]//Proceedings of Computer Graphics Workshop, Taiwan: IEEE, 2002:16-20.
- [6] 3D model search engine[EB/OL]. [2012-05-09]. <http://shape.cs.princeton.edu>.

#### 作者简介:

赵仲孟 男,(1959-),博士,副教授,硕士生导师.研究方向为信息处理新技术.

聂丽娜 女,(1986-),硕士研究生.研究方向为三维图像检索技术.

张选平 男,(1963-),副教授,硕士生导师.研究方向为人工智能、图像处理.