

基于系统级封装(SiP)的信息安全芯片集成设计

冉 彤, 白国强

(清华大学 微电子学研究所密码芯片实验室, 北京 100084)

摘 要: 为了解决信息安全系统中, 逻辑运算芯片与存储器难以实现集成的问题, 并更充分地满足信息安全系统高性能、低功耗、高可靠性的要求, 本文提出了“基于 SiP 的信息安全芯片集成”的概念及具体设计方案. 根据此方案设计实现了一款集成 CPU、Flash 存储器、密码算法芯片的小型信息安全系统的 SiP 成品实例, 该成品的功能和性能验证结果均满足系统的目标需求, 从而证实了该设计方案的可行性. 该方案也符合今后电子技术和信息安全系统的主要发展方向.

关键词: 系统级封装; 信息安全芯片; 高密度集成

中图分类号: TN43

文献标识码: A

文章编号: 1000-7180(2012)01-0010-05

The Design of Information Security Chips Integration Based on System-in-Package

RAN Tong, BAI Guo-qiang

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

Abstract: In this paper, the concept “integration of information security chips based on SiP” is proposed, in order to solve the problem that it’s hard to integrate the logic chips or blocks with the memory in security systems, while bringing better performance on high-quality, lower-power consumption and high-reliability. The detailed development flow is expounded, and a product of SiP integrating CPU, Flash memory and cryptographic chip is designed. The function and properties of the SiP product satisfy the requirement, thus certificating the feasibility of this scheme. And the scheme represents the major tendency for the electronic technology and information security system in the future.

Key words: system in package; information security chip; high-density integration

1 引言

信息安全芯片是以提供加密、认证、安全存储等信息安全服务为主要功能的一类专用芯片, 为信息在实际使用过程中提供机密性与完整性保护, 可以有效地提升信息的处理、交互与存储等环节的安全性^[1], 相比于软件防护, 具有速度快、安全性高的优势. 基于芯片级的硬件安全保护技术, 已经成为信息安全市场发展的主导趋势.

信息安全芯片通常需要 ROM 或 Flash 等非易失性存储器来存储重要的密钥数据以及程序代码,

然而, 当前面临着一个“瓶颈”问题是难以实现逻辑运算芯片与存储器的集成问题: (1) 如果采用外置的非易失性存储器, 即把逻辑芯片与独立的存储器芯片做成 PCB 板级系统, 则逻辑芯片与存储器芯片之间的数据传输通路是裸露在 PCB 板上的, 密钥等重要信息容易在传输过程中被攻击者截获, 存在着很大的安全隐患. (2) 如果采用 SoC(System on chip) 技术, 即把逻辑运算模块与存储器模块集成在一块芯片中, 虽然可以实现安全存储, 但又面临着逻辑工艺与存储器工艺难以兼容的问题. 除此之外, 由于设计规则的不同, 存储器工艺比逻辑工艺更容易带来

收稿日期: 2011-05-02; **修回日期:** 2011-06-01

基金项目: 国家自然科学基金项目(61073169)

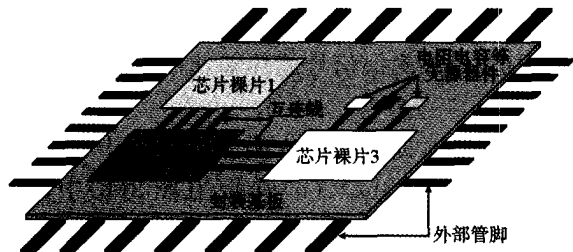
制造缺陷和可靠性问题,从而会大大降低 SOC 芯片的总成品率^[2].

系统级封装(System in Packange, SiP)可以满足信息安全芯片高性能、小体积、自主可控安全等方面的要求. 根据国际半导体技术蓝图(ITRS)的定义,“SiP 是将多个具有不同功能的有源电子器件(如 CMOS 电路、GaAs 电路等)与可选择性的电阻、电容、电感等无源器件,以及诸如微机电系统(MEMS)、光学(Optical)元件等其他元件组合在同一封装体内,成为具有系统层级功能的单个标准封装件”^[3]. 与其他芯片技术相比, SiP 具有高密度封装、多功能化设计的特点,其内部集成的各个芯片可以单独采用不同的工艺制造,从而解决不同工艺的兼容问题.

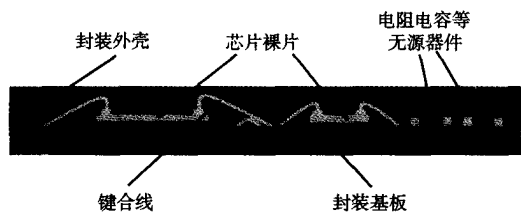
本文提出了“基于 SiP 的信息安全芯片集成”的概念,并据此实现了一款集成 CPU、Flash 存储器、密码算法芯片的小型信息安全系统的 SiP 成品.

2 SiP 的特点

图 1(a)、(b)分别是 SiP 去掉封装外壳后的结构示意图和 SiP 的横截面示意图.



(a) 去掉封装外壳的 SiP 示意图



(b) SiP 横截面示意图

图 1 SiP 的结构示意图

SiP 具有两个重要的特征:

(1) 将传统 PCB 板上的分立元件集成在一个封装体内,使系统小型化;

(2) 包含多种不同工艺、不同功能的独立芯片,以实现完整的系统功能.

与 PCB 板级系统相比, SiP 内部集成的芯片通常是裸片,从而使得器件的布局更加紧凑,缩短了芯片之间互连线的长度,减小了互连线延迟,降低了容

抗,使器件能够工作在更高的工作频率,有效地提高了系统总线的数据传输速度,并且 SiP 所集成的芯片及互连线是完全封闭在封装壳体里面的,从而使得外界无法直接探测到各芯片之间所传递信息的内容,消除了 PCB 板上信息被窃取的隐患.

与 SOC 相比, SiP 中集成的各个芯片可以单独设计与优化,不同芯片可以各自采用最合适的材料、工艺制作,从而解决了前面提到的逻辑与存储器等不同工艺的兼容问题,并且芯片的可靠性能得到大幅提高. SiP 异质芯片集成的特色,还可以将安全芯片与采用不同工艺材料实现的、能够检测不同物理量(如功耗、压力、温度、光等)的传感器集成在一起,从而实现对不同物理攻击的检测,以进一步提高安全性.

目前 SiP 技术主要应用于部分便携式电子产品中,如在手机中采用 SiP 技术集成基带模块和蓝牙模块、在相机中集成 CMOS 成像传感器等.

3 基于 SiP 的信息安全芯片集成

3.1 实验芯片型号及软件平台介绍

(1) 本实验中, SiP 所集成的三款芯片信息如下:①CPU 采用龙芯 HS3210 处理器,内嵌 32 位 RISC CPU 核,支持通用 MIPS32 指令集,主频可达 266 MHz;②存储器采用 Atmel AT45DB321 串行 SPI flash,容量为 4M * 8bit,最高工作频率 13 MHz;③密码算法芯片采用华大信安的 RSA 算法芯片 ISRSAMM11KBV1,可实现 1024、1536 和 2048 位的 RSA 算法,支持 SHA-1 和 SHA-256;密钥产生速度为:1024Bit-0.54 秒/对,2048 Bit-4.85 秒/对,最高工作频率 60 MHz.

(2) 设计工具软件采用 Cadence Allegro SPB 16.3 套件,其中调用到 SiP Digital Architect、SiP Digital Layout、SiP Digital SI、SigXplorer 等工具模块.

(3) 在 SiP 样品的功能及性能验证过程中,控制端 PC 采用 Linux Fedora 8.0 操作系统, FPGA 采用 Xilinx Spartan-3 XC3S1000.

3.2 设计方案

如图 2 所示,设计流程分为以下 8 个阶段:

(1) 分析目标需求,制定详细的系统设计规格.规格中包括各种约束信息、基板材料的选择、散热及可靠性要求等.

(2) 进行系统级电路细节设计.

此阶段需要考虑的关键问题有两个:一是基板

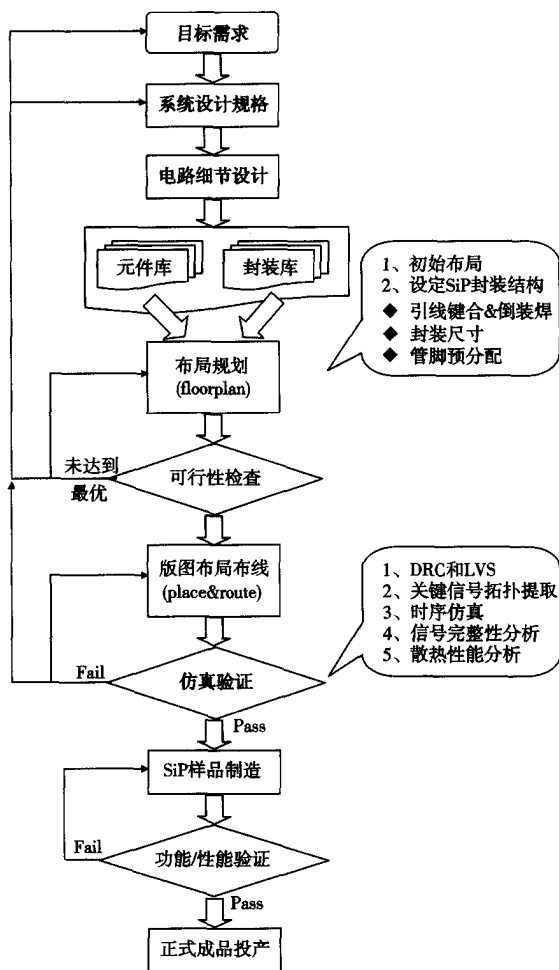


图2 信息安全芯片 SiP 集成的设计流程

上各芯片如何分布及互连,由此会涉及到信号之间的串扰、噪声、电通路的辐射等问题;二是基板上无源器件的设计,需要综合考虑无源器件工艺的限制、Q值参数、共振频率等。

(3) SiP 的布局规划 (floorplan).

此阶段定义各个有源及无源器件在基板上的布局区域,并设定封装的结构,包括:芯片与基板的连接方式采用引线键合还是倒装焊、封装的尺寸、IO管脚的数目及放置方式等,同时需要为散热量大的芯片设计接地的专用散热通道。

布局规划之后进行可行性检查,明确布局对时钟延迟的影响,决定需要端接的信号,并对电源分布系统进行早期评估。如果发现系统的性能及封装尺寸等方面可以进一步优化,则返回修改设计规格及电路细节信息,直至达到最优的效果。

(4) 物理版图的详细布局布线。

根据电气、物理等方面的约束信息,在上一阶段所定义的布局区域内放置各个元件,并进行细节布线。

布线过程中需要仔细考虑系统电路中各个部分的电流返回路程,按照不同的电压分配供电层平面与接地层平面;数字电路芯片与模拟电路芯片要设置有地线的隔离带,以降低芯片之间的串扰;一切时钟连接线都需要与其它信号线隔离,以减少 EMI 辐射。另外,需要估计各主要芯片的功耗,并应用三维模型及有限元模拟方法对 SiP 的散热性能进行分析、优化^[4-6]。

(5) 布线后仿真。

布线结束后,进行设计规则检查(DRC)。同时,提取时钟信号、CPU 输入输出信号、存储器信号等关键信号网络的实体拓扑进行仿真,以更精确的验证信号时序和波形是否满足设计要求。仿真的内容包括以下三个方面:①对时钟同步信号:仿真信号时序及信号质量,满足信号的建立时间、保持时间、过冲容限与小的振荡;②对异步信号:仿真信号质量,满足信号的单调性、过冲容限与小的振荡;③布线比较密的区域:仿真走线之间的串扰,确定不同间距的平行走线的长度容限。

针对上述可能出现的时序及信号质量等问题,从以下三个方面进行优化:①调整传输线的特征阻抗;②对布线间距做精细的调整;③调整管脚端接电阻的阻值。最终确保信号的传输速率和质量满足设计需求。

本实验中,提取的时钟-数据信号拓扑示例及仿真波形分别如图 3(a)、(b)所示。在图 3(b)中,虚线为时钟信号,实线为数据信号,信号的时序、质量均满足设计要求。

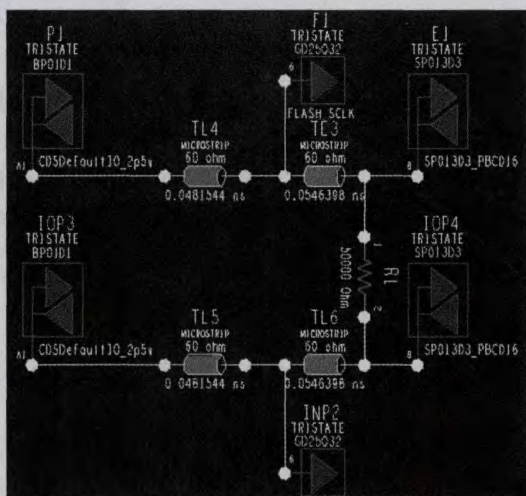
(6) 生成钻孔文件、光绘文件等,制造数据输出。图 4(a)是本实验输出的含三款芯片的 SiP 设计文件。

(7) 由封装厂家根据设计文件,进行 SiP 样品的封装制造。图 4(b)是由封装厂家制造完成的、添加封装外壳之前的 SiP 样品实物图。

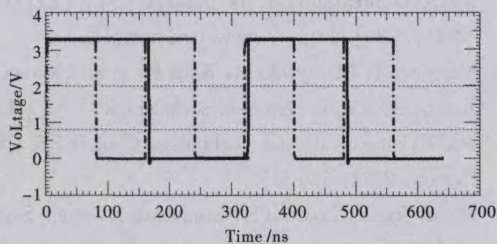
(8) SiP 样品的功能验证和性能验证。

为保证良品率,SiP 中使用的芯片通常是 KGD (known good die),即经过筛选的“已知合格芯片”。因此在 SiP 样品测试验证阶段,一般不再针对里面的单个芯片进行芯片级测试验证,而主要从系统层面进行验证。本文提出了两套验证方案。

方案一 将 SiP 样品安装在 PCB 验证板上,在 PC 控制端编写针对 SiP 样品的控制程序,通过验证板上的接口芯片与 SiP 样品进行通信,从而可以控制 SiP 样品中的芯片进行读写、加密解密逻辑运算

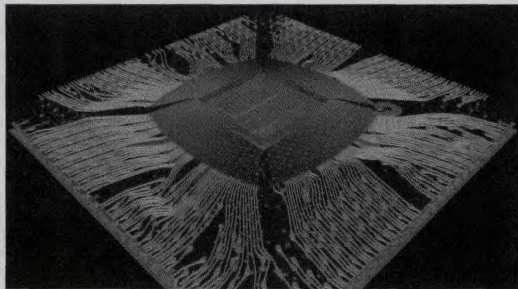


(a) 关键信号拓扑示意图

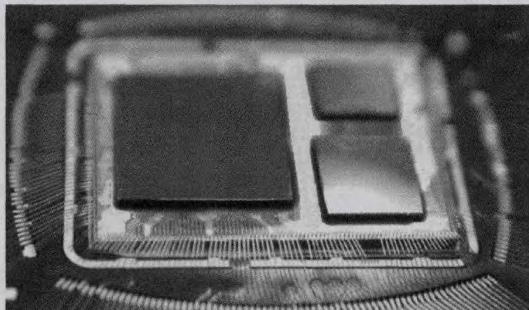


(b) 仿真波形

图3 时序和信号完整性仿真



(a) 最终的SiP设计文件



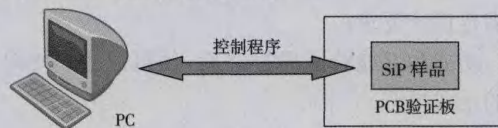
(b) 添加封装外壳之前的SiP样品实物图

图4 SiP完整设计文件及样品实物图

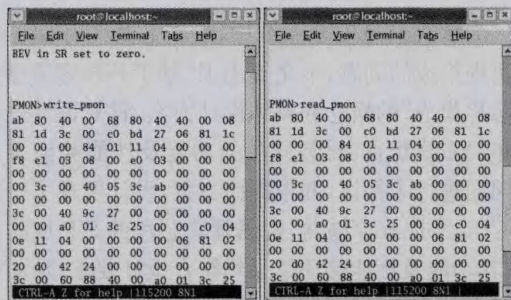
等,并将结果返回PC控制端,以观测SiP样品的功能运作是否正常。图5(a)是该方案的示意图。

本实验中,功能和性能验证的实例之一是SiP样品中CPU与Flash之间进行引导程序PMON的读写。首先,通过“write_pmon”指令,CPU将PMON写入Flash中”接下来,通过“read_pmon”指令,CPU从Flash中读取刚写入的PMON。通过比较CPU从Flash中读取到的内容与之前CPU向Flash中写入的内容是否一致,即可证实两者之前能否正常通信。图5(b)是PC控制端显示的写入及随后读取的PMON内容,可以看出CPU读取到的PMON与之前向Flash中写入的内容完全一致,从而验证了SiP样品中CPU与Flash之间可以进行正常的数据读写通信。

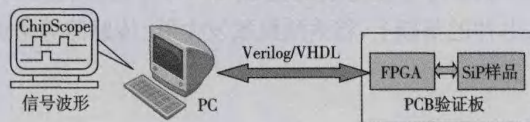
在此方案中,SiP样品返回结果的是内部芯片进行数据交互或逻辑运算的数值,因此观测起来比较直观,针对性强,但此方案不能获取实际信号的时序关系、信号完整性情况等细节信息。因此可以采用下面的第二种方案作为互补。



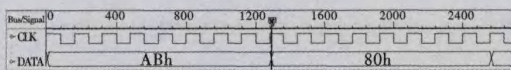
(a) 验证方案一



(b) 方案一结果示例



(c) 验证方案二



(d) 方案二结果示例

图5 功能/性能验证

方案二 鉴于FPGA的开发软件里面大多自带了在线逻辑分析仪的功能,诸如Xilinx ISE的chipscope、Altera的Signal Tap等,能够以波形图的方式对信号进行实时观测,因此本方案中,在PC

和 SiP 样品之间添加了一块 FPGA, 这样就将 PC 控制环节前移, 由 FPGA 来对 SiP 样品的功能及性能验证进行控制. 图 5(c) 是该方案的示意图.

通过在 PC 上编写 Verilog 或 VHDL 代码, 下载到 FPGA 里面, 并且将在线逻辑分析仪的 IP 核插入到 FPGA 的设计网表中, 这样就可以由 FPGA 来控制 SiP 样品中不同芯片的读写、逻辑运算等, 并将生成的信号波形显示在 PC 端的在线逻辑分析仪上, 从而可以对信号的细节波形进行实时监测. 诸如信号延迟的情况, 信号的建立时间、保持时间是否符合设计规范等等, 这样就对方案一形成了有力的补充.

以前面的 PMON 读写为例, 图 5(d) 是在 chipscope 上观察到的波形. 本实验中, SiP 组件中 CPU 与 SPI Flash 通信的时钟信号频率为 6.25 MHz, 通过将 100 MHz 的 CPU 系统时钟 16 分频得到, 因此相应的时钟周期为 160 ns, 信号的建立时间、保持时间满足设计要求.

功能和性能验证通过之后, 便可以进行 SiP 成品的正式投产.

4 结束语

为解决信息安全系统中, 逻辑芯片与存储器难以实现集成的问题, 本文提出了“基于 SiP 的信息安全芯片集成”的概念和具体设计方案. 针对设计过程中布局布线仿真、封装样品的功能及性能验证等关键问题进行了探讨, 并根据此方案, 设计实现了一款含 CPU、Flash 存储器、密码算法芯片的 SiP 成品实例, 其功能及性能验证结果均符合设计要求, 从而证明了设计方案的可行性. 接下来的工作是:

(1) 在已经完成的集成 CPU、存储器、密码算法芯片的基础上, 将真随机数发生器、传感器等集成

到 SiP 组件中来, 以实现一个更加完善的信息安全系统.

(2) 针对 SiP 组件的可靠性进行研究. 包括如何确定主要的失效机理、如何根据实验数据去评价 SiP 在预期条件下的可靠性等, 并设计 SiP 组件抗击非侵入式攻击的方案, 以进一步提高 SiP 组件的安全性.

参考文献:

- [1] 叶世芬. 安全芯片物理防护研究 [D]. 杭州: 浙江大学, 2005.
- [2] 汪东. 嵌入式存储器面面观[J]. 今日电子, 2005(12): 38-42.
- [3] ITRS. The next step in assembly and packaging: system level integration in the package (SiP) [EB/OL]. [2011-04-30]. <http://www.itrs.net>.
- [4] Miettinen J, Mantysalo M, Kaija K, et al. System design issues for 3D system-in-package (SiP) [C]//Electronic Components and Technology Conf IEEE. USA: Florida, 2004: 610-615.
- [5] Mandrekar R, Bharath K, Srinivasan K, et al. System level signal and power integrity analysis methodology for system-in-package applications [C]//Design Automation Conf. San Francisco: ACM/IEEE, 2006: 1009-1012.
- [6] Pulici P, Vanalli G, Dellutri M, et al. Signal integrity flow for system-in-package and package-on-package devices [J]. the IEEE, 2009, 97(1): 84-95.

作者简介:

冉 彤 男, (1987—), 硕士研究生. 研究方向为信息安全芯片设计.

白国强 男, (1963—), 博士, 副教授. 研究方向为信息安全芯片设计.