

基于智能卡标准的循环冗余校验码的研究与实现

许全胜^{1,2}, 吴春瑜¹, 张文婧², 王绩伟¹

(1 辽宁大学 物理学院, 辽宁 沈阳 110036; 2 北京宏思电子技术有限责任公司, 北京 100191)

摘 要: 分析了国内外智能卡应用中 CRC 校验方法的异同, 深入研究了智能卡标准及 CRC 生成多项式, 并把 CRC 的两种计算类型融合在一起, 结合智能卡标准中 CRC 校验的特点提出了一种新的 CRC 计算模块的硬件实现方法. 根据此方法完成了一种 CRC 计算模块的硬件设计, 对设计进行了 RTL 仿真验证, 通过了 FPGA 验证, 并实施了投片. 该芯片已经通过流片测试, 结果表明模块功能和性能达到设计指标, 性能良好.

关键词: 循环冗余校验码; 智能卡标准; 硬件设计

中图分类号: TN4

文献标识码: A

文章编号: 1000-7180(2011)11-0031-04

The Research and Implementation of Cyclic Redundancy Check on the Basis of Smart Card Standard

XU Quan-sheng^{1,2}, WU Chun-yu¹, ZHANG Wen-jing², WANG Ji-wei¹

(1 College of Physics, Liaoning University, Shenyang 110036, China;

2 Beijing Hongsi Electronic Tech. Co., Ltd., Beijing 100191, China)

Abstract: The article analyzed the domestic and international CRC checking methods which are applied to Smart Card, and deep research on Smart Card standard and the CRC polynomial. On this basis, the two types of CRC calculation are mixed together, and a new hardware realization method is presented combining with Smart Card standard. According to this method a hardware design of CRC calculation module is completed. The design had been simulated on RTL level, verified by the FPGA, and successfully processed. The chip has passed flow pieces tested. The results showed that the module function and performance reached design target, the performance is good.

Key words: cyclic redundancy check code; smart card standard; hardware design

1 引言

数据在传输或存储的过程中可能受到干扰而产生错误, 使接收设备收到无用的信息, 因此对通信数据进行校验是必要的. 校验的方法是在数据后面加上一个冗余信息, 这个信息是对数据的校验结果, 也称为差错检测码. 常见的差错检测码有奇偶校验位、XOR(Logical exclusive-OR operation)校验和以及 CRC(Cyclic Redundancy Check)校验和. 其中奇偶校验位、XOR 校验和都因为其不可避免的限制而不能得到最广泛的应用, 只有 CRC 校验和既可用于

数据传输过程中又可用于数据的存储过程中的差错检测. 循环冗余校验法 CRC 来自数据通信领域, 很明显地优于奇偶校验法和 XOR 法. CRC 校验和用一个 16 位的循环反馈移位寄存器产生, 反馈由生成多项式确定. 其最显著的优点是提供了对多重差错的可靠检测^[1]. 国内外的很多学者都对 CRC 的算法及硬件实现方法做了大量的研究^[2-5], 有 16 位的、32 位的、基于 FPGA 的、基于 CPLD 的、基于 USB 协议的、用 Verilog 实现、用 VHDL 实现等. 文中专门针对智能卡标准及生成多项式 $G(x) = x^{16} + x^{12} + x^5 + 1$ 进行了研究, 并把 CRC 的两种计算类型融

收稿日期: 2011-02-16; 修回日期: 2011-03-09

基金项目: 国家自然科学基金项目(10974075)

合在一起;在此基础上结合 CRC 校验的基本原理提出了一种 CRC 的硬件实现方法,进行了 RTL 仿真验证、FPGA 验证和芯片流水验证。

2 CRC 校验原理

2.1 CRC 校验基本原理

CRC 校验利用的是线性编码理论,对于要进行检验的 K 位二进制码序列,在发送端以一定的规则产生一段 R 位的校验码(即 CRC 码),附在信息后边,构成一个新的二进制码序列,共 $(N = K + R)$ 位,并发送给接收方。在接收端,根据信息码和 CRC 码之间所遵循的规则进行检验,以确定传送中是否出错。这种编码又叫 (N, K) 码。对于一个给定的 (N, K) 码,可以证明存在一个最高次幂为 $N - K = R$ 的多项式 $G(x)$,根据 $G(x)$ 可以生成 K 位信息的校验码,而 $G(x)$ 叫做这个 CRC 码的生成多项式。

CRC 校验码的具体生成过程为:将发送信息看成一个信息多项式 $M(x)$,将 $M(x)$ 左移 R 位,则可表示成 $2^R M(x)$,这样 $M(x)$ 的右边就会空出 R 位,这就是校验码的位置。通过 $2^R M(x)$ 除以生成多项式 $G(x)$ 得到的余数就是校验码。生成 CRC 校验码后将其附加在发送信息 $M(x)$ 之后发送出去。接收方的检验方法有两种,一种是针对发送的数据部分采用与发送过程同样的方法进行计算,并与接收到的 CRC 部分进行比较看是否相同;另一种是针对发送数据 $M(x)$ 和校验码部分共同构成的数据按照 CRC 生成的方法进行计算,按照有限域上的除法计算得出的结果应当是全 0。当得出了非全 0 的数据的时候就表示传输过程中发生了错误。实际的 CRC 计算中使用是模 2 多项式运算,模 2 除法与算术除法类似,但每一位除(减)的结果不影响其它位,即不向上一位借位,所以实际上就是异或运算^[6-7]。

2.2 智能卡中使用的 CRC 原理

CRC-16 的实际应用标准有 13 种之多,其中有 5 个不同的生成多项式:

- ① $x^{16} + x^{15} + x^2 + 1$ (CRC-16-IBM)
- ② $x^{16} + x^{12} + x^5 + 1$ (CRC-16-CCITT)
- ③ $x^{16} + x^{15} + x^{11} + x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ (CRC-16-T10-DIF)
- ④ $x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + 1$ (CRC-16-DNP)
- ⑤ $x^{16} + x^{10} + x^8 + x^7 + x^3 + 1$ (CRC-16-DECT)

智能卡标准中所使用的生成多项式就是 $x^{16} +$

$$x^{12} + x^5 + 1.$$

CRC 校验和计算过程如下:(1)16 位 CRC 寄存器被置入其初始值;(2)数据逐位送入反馈移位寄存器中,从最低位(或最高位)开始;(3)反馈(它表示多项式除法)经位逻辑 XOR 运算在 CRC 位上进行。当所有数据位都已经馈送至寄存器后,计算完成,而 16 位的内容即是所需之 CRC 校验和。文中后面的描述将从低位开始计算的方法定义为 Type0,从高位开始计算的方法定义为 Type1。

接收数据的一方重新计算数据的 CRC 校验和并将它和随数据发送的校验和相比较即可验证校验和。若它们是一样的,则可知数据和校验和未曾改变。另一种方法是接收方重新计算数据及其校验和,若结果为 0 则正确,否则出错。

另外,由于各个厂家智能卡的实际应用不同,CRC 的校验方法也略有不同。有的智能卡通讯设备采取了 CRC 校验码取反发送的验证机制,则 Type0 的冗余校验寄存器结果为 0xF0B8 代表校验正确;Type1 的结果为 0x1D0F 代表校验正确。

3 CRC 硬件电路的实现方法

以 Type0 为例,CRC 的算术运算过程如下:

- (1)设置 CRC 寄存器,并给其赋初始值。
- (2)将数据的第一个 8-bit 字符与 16 位 CRC 寄存器的低 8 位进行异或,并把结果存入 CRC 寄存器。
- (3)CRC 寄存器向右移一位,最高有效位(bit15)补零,移出并检查最低有效位(bit0)。
- (4)如果最低有效位为 0,重复第三步;若最低有效位为 1,CRC 寄存器与多项式码相异或。
- (5)重复第 3 与第 4 步直到 8 次移位全部完成。此时一个 8-bit 数据处理完毕。
- (6)重复第 2 至第 5 步直到所有数据全部处理完成。
- (7)最终 CRC 寄存器的内容即为 CRC 值。

CRC 计算的硬件电路可用除法电路来实现,除法电路的主体包括线性移位寄存器和异或门。线性移位寄存器一次移一位,实现除法功能,异或门完成不带进位的减法功能。如果商数为“1”,则从被除数的高阶位减去除数,同时移位寄存器右移一位,准备为被除数的较低位进行计算。如果商数为“0”,则移位寄存器直接右移一位^[8]。CRC 校验码生成器的原理图如图 1 所示。

当采用 Type1 方法时,同 Type0 方法的区别就

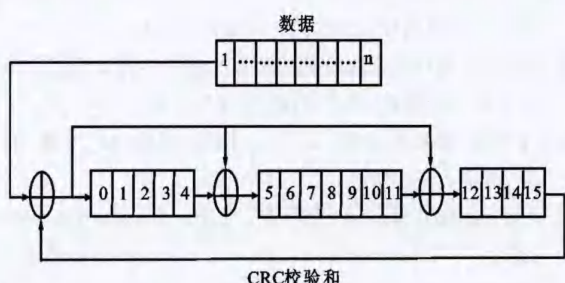


图1 Type0 的CRC 校验码生成器原理图

是数据从高位送入线性移位寄存器中和寄存器的移位方向变为向左. 其原理如图2所示.

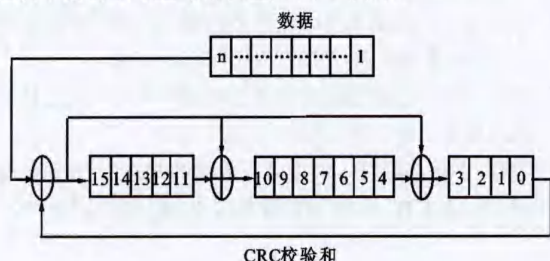


图2 Type1 的CRC 校验码生成器原理图

通过对CRC 校验基本原理的理解和对其硬件实现方法的研究,得到CRC 校验模块的结构如图3所示.

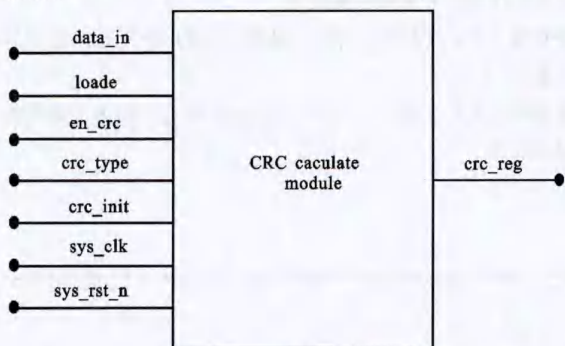


图3 CRC 校验模块结构图

各引脚的功能定义如下:

- crc_reg: CRC 校验寄存器;
- data_in: 需要计算CRC 值的数据;
- load_e: 加载CRC 初始值信号;
- en_crc: CRC 计算使能信号;
- crc_type: CRC 计算类型选择信号;
- crc_init: CRC 校验初值;
- sys_clk: 时钟信号;
- sys_rst_n: 复位信号.

4 仿真与测试结果分析

用Linux 平台上的Questasim 工具对本设计进行RTL 级仿真、门级仿真以及后仿真. 仿真结果如

图4、图5 和图6 所示.

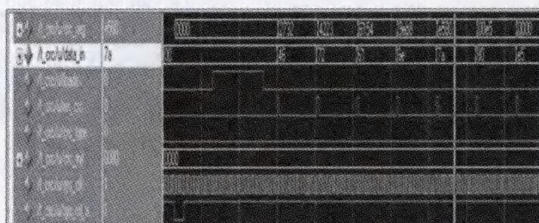


图4 Type0 校验初值为0x0000 且CRC 校验和正常发送的情况

从图4 波形可以看出,进行CRC 校验的数据依次为0x46、0x72、0x61、0x6E、0x7A, 校验和为0xE580. 把校验的低字节0x80 和高字节0xE5 依次放在数据后面进行CRC 计算后,结果变为0x0000, 符合文中第2 部分的CRC 原理.

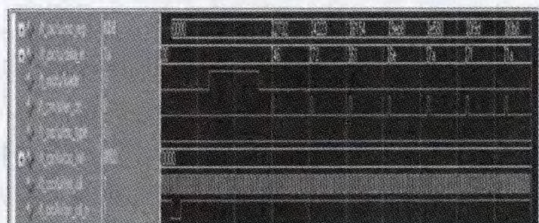


图5 Type0 校验初值为0x0000 且CRC 校验和取反发送的情况

由图5 知,计算的数据和校验和与前一种仿真情况一致,只是把校验和0xE580 取反后变成0x1A7F 再从低字节开始计算CRC 校验和. 计算结果为0xF0B8,也符合文中第2 部分的CRC 原理.

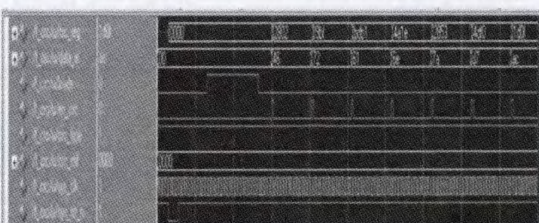


图6 Type1 校验初值为0x0000 且CRC 校验和取反发送的情况

如图6 知,计算数据和从低位开始计算的情况一致,但是发现校验和的值变为0x2853,而不是0xE580. 这是由于从高位开始计算和从低位开始计算的方式不同造成的,这种结果也是已经预见到并且符合设计目标的. 把校验和0x2853 取反变成0xD7AC,按先高后低的顺序进行CRC 计算后结果为0x1D0F,完全符合设计目标. 注意这里要先计算高字节0xD7,后计算低字节0xAC,这也是与前两种情况最大的不同点.

除以上3 种情况外,文中的设计还允许用户设

置其他的初始值,例如 0xFFFF. 和以上 3 种情况的不同点仅在于 CRC 校验和的值不同. 对于接收方来说,校验结果只有 0x0000、0xF0B8 和 0x1D0F 三种情况. 另外,从图 4、图 5 可以看出,结果完全与文献[1]中的 CRC 校验和计算的例子相符,说明本设计适用于智能卡 T=1 传输协议.

用 MedWin 开发软件进行流片测试的结果和仿真测试的一致,故本设计很好的实现了设计目标.

5 结束语

文中根据 CRC 校验和的计算原理并结合智能卡 T=1 传输协议完成了一种 CRC 计算模块的硬件设计. 由仿真测试结果可以看出,本设计能够完成 CRC 计算并检验正误,且已实际应用于一款 SOC 芯片的智能卡接口设计中. 该芯片已经通过流片测试,模块功能和性能达到设计指标,对提高芯片应用灵活性起到了很好的效果. 本设计主要是针对 CRC 的智能卡应用,对于其他的生成多项式的 CRC 校验并不适用. 但是本设计在理论上实现了两种计算方法的并用,使其更具灵活性;从实用角度还可适用于其他相同生成多项式 ($G(x) = x^{16} + x^{12} + x^5 + 1$) 的应用中,具有非常强的可移植性.

参考文献:

- [1] Wolfgang Rankl, Wolfgang Effing. 智能卡大全—智能卡的结构·功能·应用[M]. 3 版. 王卓人,王锋,译. 北京:

电子工业出版社,2002;90—91/245—248.

- [2] 蒋安平. 循环冗余校验码(CRC)的硬件并行实现[J]. 微电子学与计算机,2007,24(2): 107—109.
 [3] 王爱英. 智能卡技术—IC 卡与 RFID 标签[M]. 3 版. 北京:清华大学出版社,2009;47—51.
 [4] International Standard ISO/IEC 13239. Information technology — Telecommunications and information exchange between systems — High — level data link control (HDLC) procedures [S]. 2002.
 [5] 朱怀宏,姜永兵. 一种基于块编码的压缩视频通信差控算法[J]. 微电子学与计算机,2008,25(9): 69—71.
 [6] 黄维超,刘桥,黄初华. 基于 Verilog 的 CRC 并行实现[J]. 微计算机信息,2009,25(10):112—113.
 [7] 姚威. 循环冗余校验码并行算法的研究与实现[J]. 计算机与数字工程,2006,34(9): 112—114.
 [8] 谭华,韦林,田宜君. 32 位并行数据的 CRC—16 编码器的 FPGA 实现[J]. 河池学院学报,2008,28(2):74—79.

作者简介:

许全胜 男,(1984—),硕士研究生. 研究方向为集成电路设计与研究.

吴春瑜 男,(1953—),博士,教授,硕士生导师. 研究方向为半导体器件和集成电路设计.

张文婧 女,(1975—),博士,高级工程师. 研究方向为信号与系统.

王绩伟 男,(1968—),博士,副教授. 研究方向为半导体物理与器件.

(上接第 30 页)

- [2] 王玲,温东新,杨孝宗. 时间约束下低功耗的综合方案[J]. 半导体学报,2005,26(1):287—293.
 [3] 刘志鹏,边计年,周强. 高层次综合中基于整数线性规划模型的多目标功耗优化算法[J]. 计算机辅助设计与图形学学报,2007,19(8):966—972.
 [4] Paulin P G, Knight J P. Force directed scheduling for the behavior synthesis of ASICs[J]. IEEE Transactions on CAD, 1989, 8(6):661—679.
 [5] Allam A K, Ramanujam J. Modified force — directed scheduling for peak and average power optimization using multiple supply — voltages [C]// Proceedings of 2006 IEEE International Conference on Integrated Circuit Design and Technology. France: CotedAzur, 2006: 1—5.

- [6] Gupta S, Katkoori S. Force — directed dynamic power optimization[C]// Proceedings of IEEE Computer Society Annual Symposium on VLSI. India:Chennai, 2002: 68—73.

作者简介:

司巧梅 女,(1980—),讲师. 研究方向为电子设计自动化、信息安全.

樊持杰 女,(1974—),副教授. 研究方向为电子设计自动化、信息安全.

孙强 男,(1979—),博士,副教授,CCF 会员. 研究方向为 EDA 高层次低功耗设计和高层次可测性设计等.