DVD 伺服控制芯片中内容加扰系统的硬件结构

夏 军, 袁丽霞, 邹雪城
(华中科技大学电子科学与技术系, 湖北武汉 430074)

摘 要: 本文介绍了一种用于 DVD2ROM 伺服控制芯片的内容干扰系统(CSS)的硬件结构. 该系统通过在 DVD 驱动器和主机之间进行认证和对密钥进行加扰, 可有效防止对 DVD 盘片的非法拷贝. 用 Verilog HDL 完成整个系统的设计, 功能仿真结果表明, 设计成功. 采用 CMOS 标准单元库的综合结果为: CSS 的最大时钟频率为 100MHZ, 面积为 1.69mm^2(0.25Lm), 当 CSS 的频率为 100MHZ 时功耗为 37.38mW, 其性能足以满足 DVD 应用.

关键词: 内容加扰系统; DVD2ROM; Verilog HDL; 仿真; 综合
中图分类号: TN432 文献标识码: A 文章编号: 0372-2112 (2005) 02-0214-04

Hardware Architecture of a Content Scrambling System for DVD Servo Controller

XIA Jun, YUAN Li2xia, ZOU Xue2cheng
(Department of Electronic Science & Technology, Huazhong Univ. of Sci. & Tech., Wuhan, Hubei 430074, China)

Abstract: This paper presents the hardware architecture for a Content Scrambling System (CSS) that can be used as a building block for DVD2ROM servo controller. It is designed to prevent illegal copy of DVD disc. This includes performing the authentication between DVD drive and the host and scrambling the keys. The system has been implemented in Verilog HDL and the simulation results indicate that the design is successful. Synthesis for a 0.25Lm standard-cell library provides an estimation of 100MHZ achievable clock-frequency, 1.69mm^2 and 37.38mW power dissipation. It has sufficient performance for DVD applications.

Key words: CSS(Content Scrambling System); DVD2ROM; Verilog HDL; simulation; synthesis

1 引言

由于能够有效地防止对 DVD 光盘的非法拷贝, CSS 几乎被所有的商业 DVD 设备所使用[1]. DVD2ROM 的视频和音频数据是经过加密编码的, 加扰的源是标题密钥(Tittle Key), 同时标题密钥被光盘密钥(光盘密钥)加密, 主机在播放影碟的时候必须拿到这两个密钥才能顺利播放[2,3]. 在密钥从 DVD 驱动器传送到主机的过程中, 为了保证数据传输通道的安全性, 即保证光盘密钥和标题密钥能够被安全地传输, CSS 建立了一道认证机制(Authentication Mechanism)[4], 通过总线密钥(BUS KEY)对光盘密钥和标题密钥进行加扰.

当 DVD 播放机读取数据时, 伺服控制芯片中的 CSS 将进行复杂的密码校验. 如果密码校验成功, 数据才可以还原成 MPEG2.2 格式和转换为视频信号和音频信号. 本文介绍了一种完成认证过程、光盘密钥和标题密钥的加扰和传输的 CSS 的设计, 它用于 DVD 伺服控制芯片中.

2 CSS的原理及系统分析

根据 DVD 标准以及 CSS 的相关的规范[5], CSS 主要包含两部分:

(1) DVD 驱动器和主机之间的授权认证; 如图 1 所示.

其认证流程为: 主机发送一个随机码流到驱动器, 驱动器对其加密后返回主机, 主机解密后确认是否和原码流相同, 如果相同则驱动器被授权. 主机的授权过程与驱动器的授权过程相同. 交互授权的结果是产生总线密钥用于对在主机和驱动器之间传输的数据进行加密. 只有主机和驱动器可以产生用于解密的密钥.

(2) 光盘密钥和标题密钥的加扰. 加扰过程为:

(a) 驱动器用总线密钥对光盘密钥和标题密钥加扰. CSS 对密钥的加扰开始于伺服控制芯片从 DVD 光盘读取包含光盘密钥和标题密钥的扇区数据. 数据先读入 UPI(微处理器接口)寄存器然后传送到到存储区管理模块(BM2Buffer Manager)并生成 CSS 内存指针以用于 CSS 读取数据. CSS 从 BM 中一次读取一个字节的密钥, 加扰后储存到 BM 中由微处理器内存指针所指向的区域. 密钥加扰完成后, CSS 发出 CSS_DONE 中断.

(b) 通过微处理器内存指针, UPI 寄存器读取加扰后的密钥并传送至主机.

收稿日期: 2003-10-18; 修回日期: 2004-10-09

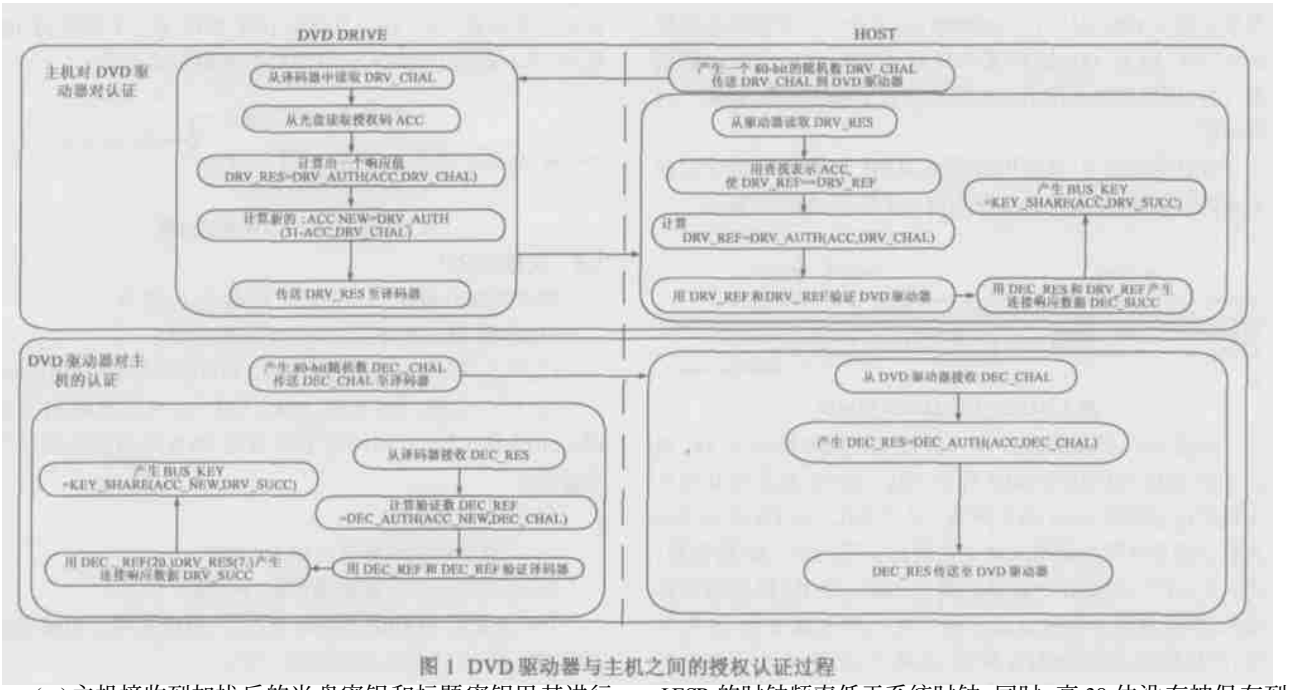

图 1 DVD 驱动器与主机之间的授权认证过程

(c) 主机接收到加扰后的光盘密钥和标题密钥用其进行解扰. 采用正确的光盘密钥和标题密钥主机可对光盘上的音频、视频数据解扰.

3　CSS 的系统结构及主要模块硬件实现

311　CSS 系统结构

图 2 表示 CSS 系统结构图, 它由四个模块组成:

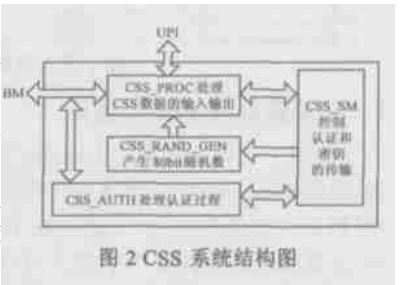

图 2 CSS 系统结构图

(1) CSS_PROC: 处理 CSS 数据输入输出, 它是 CSS 与 DVD 伺服控制芯片中 BM 和 UPI 的接口.

(2) CSS_RAND_GEN: 产生 80bit 伪随机数用于 DVD 驱动器对主机的认证, 伪随机数的产生用到了 42 位线性反馈移位寄存器(LFSR2Linear Feedback Shift Register).

(3) CSS_AUTH: CSS 中最为关键的认证运算模块.

(4) CSS_SM: 控制 CSS_AUTH 模块的认证过程, 并且在 CSS_PROC 中开启密钥传输.

由以上这些模块构成的 CSS 系统实现 DVD 驱动器和主机之间的交互授权认证以及光盘密钥和标题密钥的加扰两大功能, 系统时钟为 100MHZ.

312　模块 CSS_RAND_GEN 硬件结构

根据规范/ 用于 DVD2ROM 驱动器中认证器的内容加扰系统0, 随机数发生器能够为任何高于 41 位线性复杂度的伪随机数发生器[7].

本设计中, 发生器由 42 位的线性反馈移位寄存器(LFSR2Linear Feedback Shifter Register) 和随机组合逻辑组成, 输出为 80 位, 其中随机组合逻辑用于产生高 38 位. 为了节省功耗, LFSR 的时钟频率低于系统时钟. 同时, 高 38 位没有被保存到寄存器中以节省面积. 图 3 表示了模块 CSS_RAND_GEN 的结构.

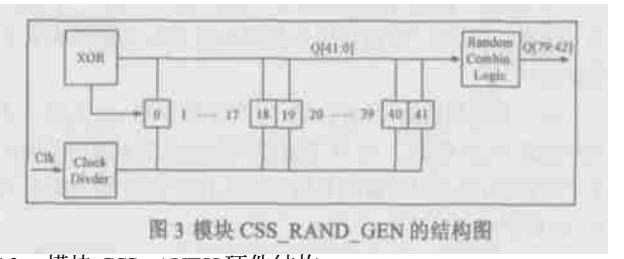

图 3 模块 CSS_RAND_GEN 的结构图

313　模块 CSS_AUTH 硬件结构

CSS 最关键的地方在于主机和 DVD 驱动器之间的认证, 因而认证运算模块 CSS_AUTH 成为设计重点. 根据图 1 的认证过程, 它由 5 个子模块来完成, 如图 4 所示.

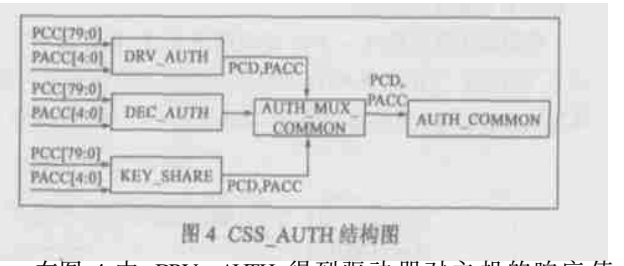

图 4 CSS_AUTH 结构图

在图 4 中, DRV_AUTH 得到驱动器对主机的响应值 DRV_RES, 返回到主机以完成主机对驱动器的认证并产生总线密钥. 而 DEC_AUTH 则和 KEY_SHARE 共同完成驱动器对主机的认证: DEC_AUTH 取回主机对驱动器的响应值以后, 通过和主机相反的过程得到一个参考值, 将它和 DEC_RES 比较后验证主机, 验证成功产生连接数, 送给 KEY_SHARE 最终产生用以加密的总线密钥. 为了使 CSS_AUTH 的面积最优, 如图 3 所示, 将 CSS_DRV_AUTH、CSS_DEC_AUTH 和 CSS_KEY_SHARE 三个模块中共同包含的逻辑部分抽出形成一个

单独的模块 CSS. AUTH. COMMON, 同时设计一个多路选择模块 AUTH. MUX. COMMON 来选择到 AUTH. COMMON 的数据源. 这种模块多路复用结构很好的节省了电路面积, 提高了运算速度.

在这些模块中, 被复用的模块 AUTH. COMMON 包含着最复杂的数据路径, 设计时划分为四个子模块, 如图 5 所示:

图 5 AUTH_COMMON 结构图

在图 5 中, KEY 模块中存放通过 LICENSE 得到的 AK, 通过 XOR 模块与 PCD[79:40] (对于 DRV. AUTH 来说 PCD 为从主机发送过来的 80bit 随机码流; 对于 DEC. AUTH 来说 PCD 为驱动器自身产生的用以对主机进行认证的 80. bit 随机数; 而对于 KEY. SHARE PCD 来说则为 DEC. AUTH 模块的运算结果, 即驱动器对主机认证过程产生的中间连接数) 进行异或, 然后经过 SCHEDULER 模块(由两个 LFSR、一个一位全加器和一些 XOR 门及寄存器组成) 得到 IAK, 最后送到 SUBSTITUTOR 模块得到 AUTH 三个子模块各自的运算结果.

3.4 模块 CSS. PROC 硬件结构

模块 CSS. PROC 被划分为两个部分: 第一个部分用于读/写 CSS 寄存器, 第二个部分用于传递加扰后的光盘密钥和标题密钥.

对于单周期的读/写寄存器, 实现非常简单. 然而对于多周期的读/写寄存器, 一个字节偏移计数器被用于指向不同的字节偏移量, 这是因为数据总线仅为 8 位而寄存器位宽为 40 位/80 位之一.

对于密钥传递过程, 采用了两个计数器. 一个用于计数从一个扇区的数据区域有多少个字节从 BM 中被读出, 另一个用于当总线密钥被加扰时控制其字节偏移量. 在密钥传递期间, 从 CSS 到 BM 的一个数据请求信号将维持在高电平直到所有的字节都被接收完.

密钥的加扰过程在一个时钟周期内完成. 寄存器 BUS. KEY. OFFSET. CNT 选择 40 位的总线密钥的字节偏移量并将其与从 BM 来的 8 位数据相异或, 其结果在下一个时钟周期被送至寄存器 CSS. BM. DATA. OUT 并在下一个周期被 BM 取来. 图 6 表示了模块 CSS. PROC 的密钥加扰过程.

图 6 CSS_PROC 密钥加扰过程

3.5 状态机设计

根据系统分析, CSS 有 6 种工作模式, 分别为:

(1) 计算 DVD 驱动器的响应值 DRV. RES.

(2) 产生对主机认证的呼叫 DEC. CHAL 用于对主机的认证.

(3) 产生主机的参考值 DEC. REF, 并与主机的响应值 DEC. RES 作比较, 若相同则主机通过 DVD 驱动器认证并产生连接数.

(4) 产生总线密钥.

(5) 用总线密钥对光盘密钥进行加扰.

(6) 用总线密钥对标题密钥进行加扰.

CSS 中采用 MOORE 类型的状态机, 围绕这些工作模式进行状态转换. 其状态转换图如图 7 所示.

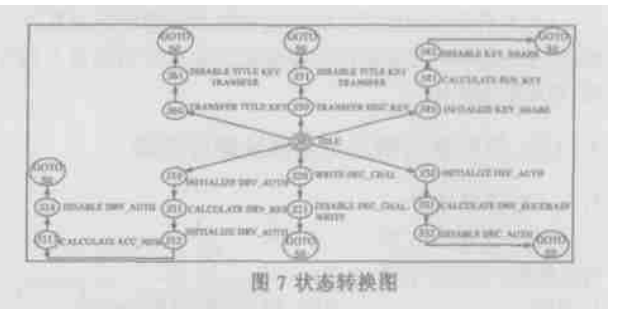

图 7 状态转换图

4 功能仿真和 FPGA 验证

按照上述设计思想, 用 Verilog HDL 对 CSS 进行 RTL 描述. 使用 Synopsys VCS 对其 6 种模式进行仿真, 通过 Debussy 的 PLI 接口生成波形文件(. fsdb), 在 Debussy 中对波形进行分析. 光盘密钥共有 2048 个字节, DVD 扇区中包含光盘密钥的数据区在第 13 个到 2060 个字节. 在测试脚本里预先设定总线密钥的值并导入 2352 个字节的 DVD 扇区数据到 BM 以便对 CSS 进行功能测试. 在这里只针对光盘密钥加扰模式的仿真波形进行说明. 仿真波形如图 8 所示:

图 8 光盘密钥加扰模式仿真波形

其中, CSS. BM. RD. REQ. CNT 为 CSS 向 BM 发出的读请求信号, DISC. KEY. XFER. EN 为光盘密钥传输使能信号, 均为高电平有效. BM. CSS. DATA[7:0] 为光盘密钥数据, 存储于 BM 的 FIFO 中. 当上述两个使能信号都为/10 时, 光盘密钥就从 BM 传输至 CSS 中, 每个时钟周期传送一个字节. TOTAL. OFFSET. CNT 是从 BM 传输来的数据的总的字节偏移量, 当 TOTAL. OFFSET. CNT= 11 时 DISC. KEY. START. LOC 置位, 标志着开始加扰光盘密钥. 每传送一个字节数据的光盘密钥, 就用总线密钥对其进行异或运算, 并在下一个时钟周期将加扰的结果送出并产生数据有效标志. 分析 CSS. BM. DATA.

OUT[7:0] 可知, 总线密钥 对光盘密钥进行了正确的加扰及传输.

5　实现结果

采用 Synopsys Design Complier 来实现 CSS, 工艺库为 0.25Lm CMOS 工艺库(3层金属线, 2.75V). 表1为综合结果.

表1　CSS 综合结果

模块	延迟(ns)	功耗(mW)
CSS_RAND_GEN	0.46	0.377
CSS_AUTH	0.55	15.512
CSS_PROC	1.33	15.108
CSS_SM	1.07	0.321

综合结果显示, CSS 最大时钟频率为 100MHZ, 与当前各种主流 DVD 伺服控制芯片的速度相当. 其面积为, 其中用于布线. 当 CSS 的频率为 100MHZ 时功耗为 37.38mW.

6　结论

本文介绍了一种内容干扰系统(CSS)的设计和实现. 在分析了其工作原理和系统结构后我们给出了数据通路和状态机的设计方法, 重点说明了 SUBSTITUTOR 的设计, 这是整个系统设计中的难点. 该系统在 DVD 伺服控制电路中的应用表明, 它确保了 DVD 驱动器到主机的光盘数据传输通道的安全性, 可以有效防止对 DVD 盘片的非法拷贝, 达到了设计要求.

参考文献:

[1] J A Bloom, I J Cox, T Kalker, et al. copy protection for DVD video [A]. Proceedings of the IEEE Special Issue on Identification and Protection of Multimedia Information[C]. NJ: Prentice Hall, Inc., 1999. 1267-1276.

[2] L Jean Camp. DRM: doesn. t really mean digital copyright management [DB/OL]. http://www.csc.ncsu.edu/faculty/yu/courses/csc591d/handouts/drm.ppt, 2002-11-10.

[3] ASUS eMagzine. Multimedia2DVD copy protection [DB/OL]. http://www.asusemag.com.tw/fundamental/ch15/ch15-1.html, 2002-12-7.

[4] DVD Copy Control Association. Content scrambling system (CSS) [DB/OL]. http://www.dvdcca.org/css/, 2000-11-3.

[5] ISO/IEC 16449. DVD specifications for read-only disc, part1; physical specification[S].

[6] ISO/IEC 9660. DVD content scramble system for authenticator on DVD2ROM[S].

[7] Frank A. Stevenson. Cryptanalysis of content scrambling system [DB/OL]. http://www22.cs.cmu.edu/dst/DeCSS/FrankStevenson/analysis.html, 2001-03-8.

作者简介:

夏　军　男, 1974 年 4 月出生于湖北省红安县, 现为华中科技大学电子科学与技术系博士研究生, 研究方向为计算机系统结构和 SOC 设计方法学. E2mail: hakun2002@163.com.

袁丽霞　女, 1977 年 11 月出生于湖北省蕲春县, 现为华中科技大学电子科学与技术系硕士研究生, 研究方向为模拟集成电路设计.

邹雪城　男, 1964 年 12 月出生于湖北省监利县, 现为华中科技大学电子科学与技术系教授、博士生导师, 研究方向为专用集成电路设计.