文章编号：2095-2163(2020)06-0113-04 中图分类号：TP39 文献标志码：A

DSP 中存储保护单元的设计与断言验证

肖海鹏[1]，谢海情[1]，汪 东[2]
（1 长沙理工大学 物理与电子科学学院，长沙 410005；2 湖南毅梁微电子有限公司，长沙 410005）

摘 要：针对 X-DSP 存储空间的访问安全问题，本文采用硬件保护原理设计了一个存储保护单元，通过检查访问请求属性是否安全来决定是否允许未授权用户访问存储保护区域，从而实现存储空间的数据保护功能。采用 System Verilog Assertions 编写存储保护单元的功能属性描述，并采用断言验证方法完成存储保护单元的形式化验证。在 X-DSP 芯片验证环境下，采用 FPGA 原型验证，完成存储保护单元的功能测试。结果表明，存储保护单元实现了 X-DSP 存储空间的数据保护，防止非法程序破坏安全空间，阻止未经授权的用户访问存储空间。另外，断言验证方法保证了功能验证的完备性，从而缩短了产品开发周期。

关键词：存储保护单元；断言验证；DSP；功能验证

Design and assertion verification of storage protection unit in DSP

XIAO Haipeng[1], XIE Haiqing[1], WANG Dong[2]
(1 School of Physics & Electronic Science, Changsha University of Science & Technology, Changsha 410114, China;
2 Hunan Great-leo Microelectronic Co.Ltd, Changsha 410005, China)

【Abstract】 Aiming at the access security problem of X-DSP storage space, this paper adopts the principle of hardware protection to design a storage protection unit, and decides whether to allow unauthorized users to access the storage protection area by checking whether the access request attribute is secure, so as to realize the data protection function of storage space. The System Verilog Assertions is used to write the functional attribute description of the storage protection unit and Assertions are used to complete the formal verification of the storage protection unit. In the x-DSP chip verification environment, FPGA prototype verification was used to complete the functional test of storage protection unit. The results show that the storage protection unit realizes data protection of X-DSP storage space, prevents illegal programs from destroying the security space and prevents unauthorized users from accessing the storage space. In addition, the assertion verification method guarantees the completeness of functional verification, thus shortening the product development cycle.

【Key words】 memory protection unit; assertion-based verification; digital signal processor; formal verification

0 引 言

数字信号处理器(Digital Signal Processor,DSP)广泛应用于雷达、声纳、数字通信以及语音视频信号处理[1]。为保证 DSP 能够正常有序工作，防止某些非法访问或操作破坏 DSP 的存储空间，需在 DSP 中加入存储保护功能[2-3]。

存储空间的数据保护方法有两种：软件保护和硬件保护。软件保护是 DSP 中没有集成硬件模块或有硬件模块但不使用，只依靠软件来保护存储空间，但软件保护严重影响 DSP 的处理速度；硬件保护是 DSP 中集成有专门检测和限制对存储空间访问的硬件，访问请求需要按照其属性接受存储保护单元的检测，一旦用户访问存储保护区域但不具有访问权限则产生指令预取中止和数据访问中止。

功能验证是数字集成电路设计中至关重要的环节，主要有模拟仿真验证和形式化验证两种[4-6]。随着芯片规模和复杂度的增加，模拟仿真验证存在测试向量完备性差的缺点。而形式化验证基于严格的数学模型和严密的推理与证明，遍历待测设计的整个状态空间，具有很好的完备性[7]。其中，断言验证是用于性质(属性)检验的一种常用的形式化验证[8-10]。

为了实现访问请求的属性检查，本文设计一个存储保护单元，通过检查访问请求是否取自于存储保护区域，请求访问的目的地址是否属于存储保护区域以及存储空间是否受到 CSM(Code Secure Model)保护三方面的信息，来决定是否允许用户访问存储保护区域，实现存储空间的数据保护功能。另外，为保证功能验证的完备性，采用断言验证完成存储保护单元的功能验证，并在 X-DSP 全芯片环境下采用 FPGA 原

基金项目：湖南省教育厅基金资助科研项目(17B007)；长沙市科技计划重点项目(kq1901102)。

作者简介：肖海鹏(1995-)，男，硕士研究生，主要研究方向：数字 IC 前端设计及验证；谢海情(1982-)，男，博士，副教授，硕士生导师，主要研究方向：微光电子器件与系统集成、专用集成电路设计。

收稿日期：2020-03-14

型验证,完成存储保护单元的功能测试。

1 存储保护单元设计

本文设计的 X-DSP 存储保护单元功能框图如图 1 所示,主要包括:代码安全模块 CSM、Memory Controller 模块以及 CPU_Core 模块。代码安全模块 CSM 实现从片上 Flash 读取密码并作全 0、全 1 判断以及与密匙寄存器进行密码匹配,输出结果 CSM,其值为 1 时,X-DSP 受 CSM 保护,反之,则未受 CSM 保护。Memory Controller 模块实现安全属性检查,输出安全属性标签给 CPU_Core 模块。CPU_Core 模块实现相应的 CPU 功能以及安全属性检查,以检查结果决定是否允许用户访问存储保护区域,用安全属性标签来决定是否产生指令预取中止和数据访问中止。

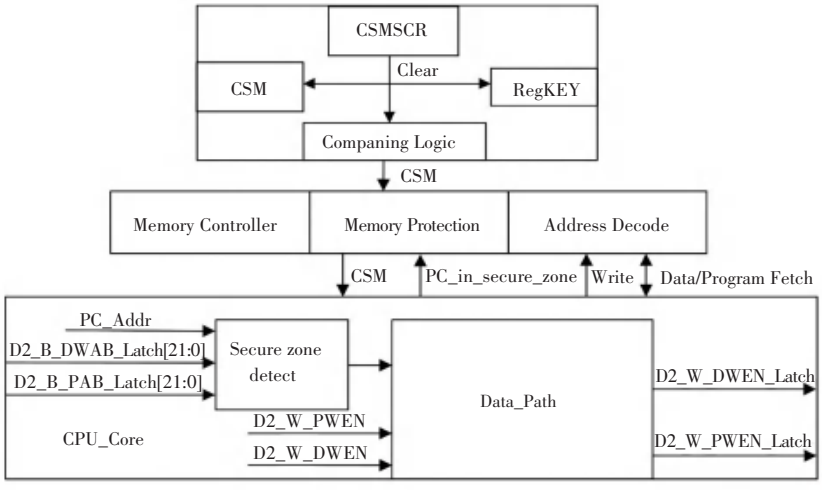

图 1 存储保护单元功能框图

Fig. 1 The formal structure diagram of memory protection unit

其工作原理:存储保护单元检查三方面的信息:(1)存储空间是否受 CSM 保护。(2)访问目的地址是存储保护区域还是非保护区域。(3)请求本身属性是安全还是不安全,即产生请求的指令是取自于保护区域还是非保护区域。如果请求本身是安全的,访问目的地址位于存储保护区域,则放行;如果请求本身是不安全的,但访问目的地址位于存储保护区域,则阻止;而对非保护区域的访问请求则不做检查。

此外,在调试仿真器连接 X-DSP 时,如果 CSM 为 0,对调试软件的请求、访存地址是非保护区域以及取指请求不做检查。如果 CSM 为 1 时,调试软件通过 JTAG 方式访问存储空间被阻止,产生 Disconnect 的命令脉冲送给调试软件并断开仿真器连接。

2 存储保护单元的断言验证

2.1 验证平台

存储保护单元的断言验证流程如图 2 所示。其中,形式属性验证工具 FPV App 完成存储保护单元的断言验证,验证所编写的功能属性在存储保护单元的 RTL(Register Translation Level,RTL)代码设计中已实现了属性所描述的功能。

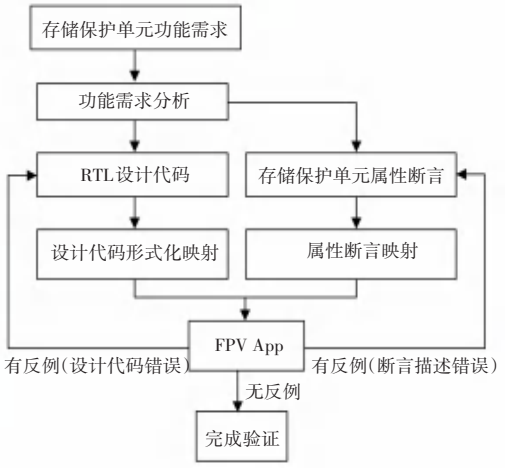

图 2 存储保护单元的断言验证流程

Fig. 2 Assertion-based verification flow of memory protection unit

2.2 功能属性

编写存储保护单元功能属性并断言,验证以下功能属性点:(1)检查请求访问目的地址是否属于存储保护区域,输出安全属性标签。(2)当请求是由存储保护区域发出,并且访问目的地址是存储保护区域,则放行。(3)当请求不是存储保护区域发出,但访问目的地址是存储保护区域,CSM 为 1 时,阻止,CSM 为 0 时,放行。(4)访问目的地址不是存

储保护区域时，则不做任何检查。（5）Memory Controller 根据 CSM 和安全属性标签控制片选信号的输出，即是否允许用户访问存储保护区域。（6）根据安全属性标签与 CSM 来控制调试仿真器的访问请求。属性建立步骤如图 3 所示。

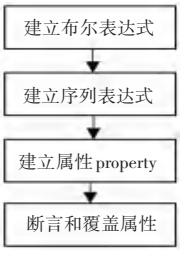

图 3　属性的建立步骤

Fig. 3　The building flow of the property

采用 System Verilog Assertions 属性描述语言编写存储保护单元的功能属性并断言，如例 1 所示。

例 1：property one；

pwl_key_true |-> ! CSM.CSM && ! CSM.ECSL；

endproperty

assert_one：assert property（one）；

cover_one：cover property（one）；

例 1 中，属性 one 根据代码安全模块的 PWL 密码与密匙寄存器值匹配成功信号 pwl_key_true 为 1 时，在当前时钟周期内检查 CSM 信号与 ECSL 信号是否为 0（CSM 与 ECSL 初始值为 1）。

2.3　验证结果与分析

编写脚本运行 FPV 工具，工具自动遍历存储保护单元的所有状态空间，验证所编写的功能属性是否正确以及功能是否实现。存储保护单元的断言验证结果如图 4 所示。结果显示，所编写的功能属性有 42 条，均被验证通过，并且编写的功能属性描述正确且在 RTL 代码设计中已实现属性所描述的功能。

3　FPGA 原型验证

FPGA 原型验证测试平台如图 5 所示，将 X-DSP 全芯片代码映射至 FPGA，采用 TI CCS 调试软件作为测试工具，使用 XDS 仿真器与 FPGA 相连，通过 CCS 软件调试操作来验证存储保护单元的物理实现。

FPGA 原型验证结果如下：X-DSP 上电复位，编写测试程序写入存储空间，当 CSM 为 0 时，存储空间未受到保护，单步执行测试程序，其结果如图 6 所示，程序运行成功，存储空间数据可以正常访问。在图 7 中。通过 CCS 调试软件的 program 操作设置密码后，CSM 变为 1，存储空间受 CSM 保护。这时，重新单步执行测试程序，JTAG 访问请求被阻止，产生了 Disconnect 的命令脉冲送给调试软件，致使调试仿真器断开连接。

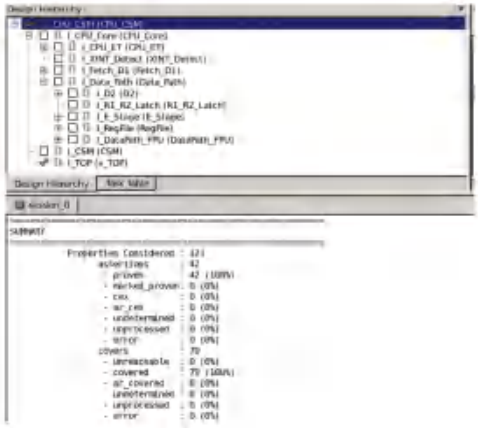

图 4　存储保护单元的断言验证结果

Fig. 4　The result of memory protection unit assertion - based verification

图 5　FPGA 原型验证测平台

Fig. 5　The testing platform of FPGA prototype verification

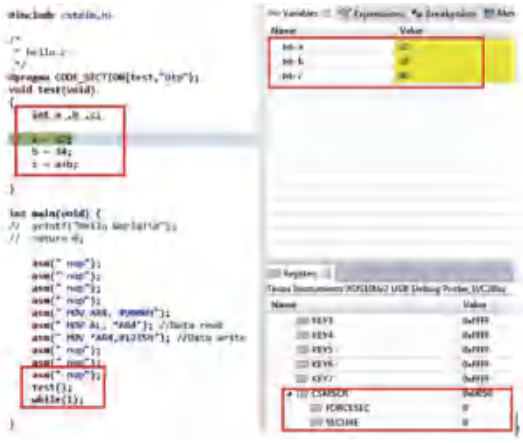

图 6　CSM=0 时程序运行结果

Fig. 6　The program running result of CSM=0

图 7　CSM=1 时程序运行结果

Fig. 7　The program running result of CSM=1

（下转第 119 页）