

基于 UVM 验证方法学的 AES 模块级验证

田 劲, 王小力

(西安交通大学 微电子学系, 陕西 西安 710049)

摘 要: 分析了基于 SystemVerilog 语言的 UVM(Universal Verification Methodology)高级验证方法学, 并使用该方法学对 AES(Advanced Encryption Standard)模块进行了功能验证. 验证结果表明, 此验证平台能够实时监测覆盖率, 控制验证进程, 优化验证事务. 该方法提高了验证的效率验证平台的可重用性, 较好地满足了芯片验证需要.

关键词: UVM 验证方法学; System Verilog; AES; 随机约束

中图分类号: TN4

文献标识码: A

文章编号: 1000-7180(2012)08-0086-05

AES Module Level Verification Based on UVM

TIAN Jin, WANG Xiao-li

(Department of Microelectronics, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: This paper analyzed an advanced verification methodology called UVM which based on system verilog language and verified the function of AES. As a result of verification, we can monitor coverage, control the platform and optimize the testbench and testcase. This Methodology can improve the verification efficiency and platform reuse. It well meets the needs of chip verification.

Key words: UVM; System Verilog; AES; Random Constraint

1 引言

随着集成电路设计向超大规模发展, 芯片验证工作的难度在不断增大, 验证的工作量已经占到整个 SOC 研发的 70% 左右, 因此提高芯片验证的效率已变得至关重要^[1]. UVM 验证方法学由 Accellera 组织于 2010 年推出, 它是一套吸收了 OVM (Open Verification Methodology)、VMM (Verification Methodology Manual) 和 AVM (Advanced Verification Methodology) 等诸多当前主流验证方法学优点的、成熟的、开源的验证方法学. UVM 采用了最佳的验证框架去实现覆盖率驱动验证, 其有效结合了测试随机产生、自测试平台和随机化约束等特点, 能大大缩短验证时间.

高级加密标准 (Advanced Encryption Standard, AES), 又称 Rijndael 加密法, 是美国联邦政府

采用的一种区块加密标准, 目前 AES 标准已成为对称密钥加密中最流行的算法之一^[2]. AES 加密数据块和密钥长度可以是 128 比特、192 比特、256 比特中的任意一个. AES 加密和解密过程有密钥扩展以及很多轮的循环和变换. 本文将以一个 8 通道的 AES 模块作为验证对象, 使用 UVM 验证方法学, 对其进行加密和解密过程的验证.

2 UVM 验证平台

UVM 验证平台由一系列可重用的称之为通用验证部件 (Universal Verification Component) 的组件组成, 这些通用验证部件具有可配置性、封装成型、易于使用、可重用性高等诸多优点, 每一个通用验证部件都拥有固定的结构, 包括了一系列的组件去完成针对某一特定协议标准的仿真、检查、采集覆盖率^[3]. 这些部件是 UVM 验证平台的重要组成部分

收稿日期: 2011-12-12; 修回日期: 2012-02-19

基金项目: 国家自然科学基金项目 (61172040)

分^[4-5].

图 1 所示为一个典型的 UVM 验证平台. 首先, 在环境部件中, 例化了一个监控部件, 一个配置模块和四个功能部件. 监控部件负责整个验证环境的功能覆盖率监测; 配置模块完成对验证环境中各个部件的配置; 四个功能部件各自完成不同的功能, 每个部件中都有独立的定序器. 驱动部件和监控部件. 在每一个功能部件中, 定序器通过传输级模型 (Trans-

action Level Model) 将随机约束好的数据项目序列发送给驱动部件, 驱动部件将这些数据项目按照一定的协议标准驱动验证对象的输入信号, 同时监控部件会按照相应的协议标准对验证对象的输入输出信息进行采样, 并将采样的结果传输给环境部件外的比对部件. 一般比对部件会采用一定的方式对采样数据的正确性进行判断.

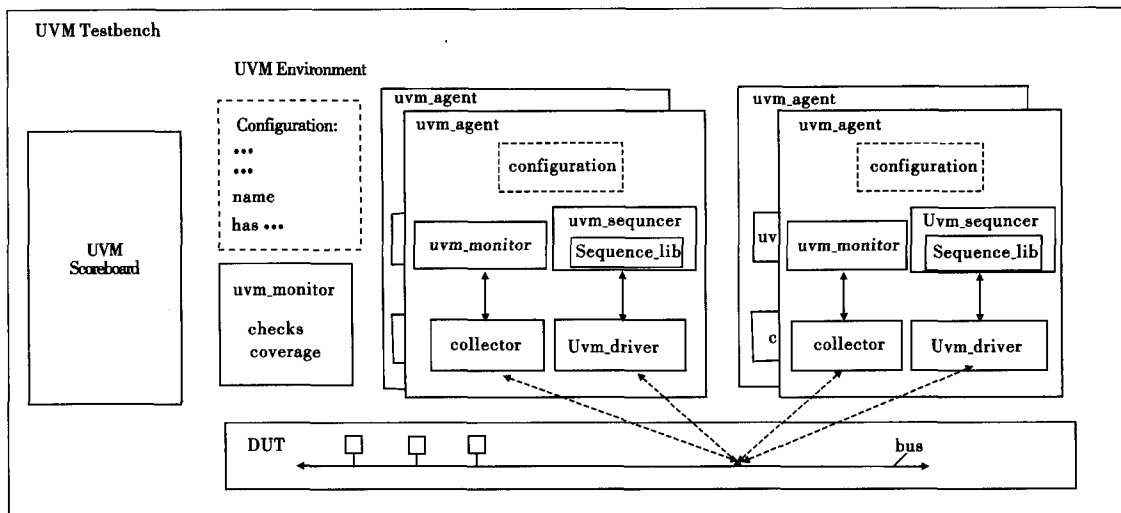


图 1 典型的 UVM 验证平台

3 AES 模块

本 AES 模块是基于 AES 算法的一个 8 通道的多模式的加密解密模块. AES 模块的结构图如图 2 所示. 该模块的八个通道共享一个 AES 核心加密解密模块, 在 AES 核心模块中有一个仲裁器采用 round robin 轮排法对八个通道的数据请求进行仲裁, 并且还有两个加密解密引擎对数据进行高效的交替加密解密. 每一个通道都有独立的一套加密解密信号, 可配置不同的加密解密方式和密钥长度.

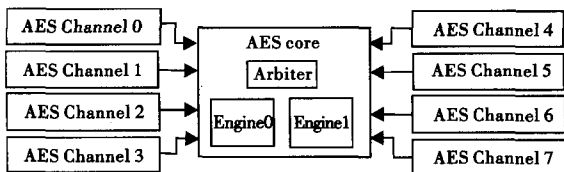


图 2 AES 结构图

该 AES 模块支持多种工作模式, 在正常工作模式下, 该模块支持 XTS 和 ECB 模式, 在特殊模式下, 该模块支持 LPA 模式, 此外此模块还能对数据进行 CTS 加密解密.

该 AES 模块的加解密数据结构图如图 3 所示.

在 AES 模块中, 最小的加密或解密的数据单元称为 128 比特的数据块 (Data Block), 多个数据块可以组成一个数据单元 (Data Unit), 为提高加密解密的效率, 该 AES 模块每次对一个数据单元的数据进行加解密, 从而完成对一个数据流 (Data Stream) 的加解密. 一个数据单元中所有的数据块共用一个 128 比特的哈希密钥 (hash key) 和一个非负整数的密钥, 这个哈希密钥在数据单元内部对于每个 128 比特数据来讲是从一个任意的非负整数开始的连续的值.

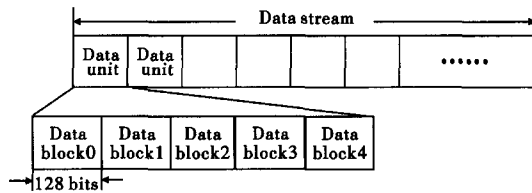


图 3 AES 加解密数据结构图

4 基于 UVM 的 AES 验证平台搭建

4.1 AES 模块验证策略

该 AES 验证的基本思路是使用随机约束激励与自动检测比较的思路, 验证策略如图 4 所示. 首先将 AES 数据项目中的变量做随机约束, 然后将该数

据项目传输给 AES 驱动部件; AES 驱动部件使用随机约束好的数据去激励 AES 模块的输入信号; 同时 AES 监控部件一方面采样驱动部件对 AES 模块的激励信息, 将该信息用于驱动 AES C 模型, 另一方面 AES Mo 驱动部件采样 AES 模块的输出信号, 将其打包传输给 AES 比对部件中; AES 比对部件获得由 AES C 模型发送的期望数据和 AES 监控部件发送过来的 AES 模块输出采样信息, 比较两者的一致性来判断验证场景的正确性。

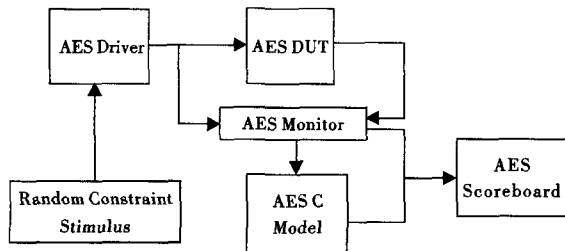


图 4 AES 验证策略

4.2 基于 UVM 的 AES 验证平台

基于 UVM 验证方法学的 AES 验证的平台如图 5 所示。AES DUT 是待验证的验证对象, 它是通过 AES Interface 和 AES_monitor, AES_driver 通信实现信息的驱动和采样的, 由于 AES DUT 有 8 个加密和解密通道, 所以在验证环境中例化了 8 个 AES_agent, 每个 AES_agent 都可以独立的驱动一个 AES 通道。8 个 AES_monitor 将采样的数据通过 TLM 传输给 AES scoreboard 中, AES scoreboard 中有 AES C Model, 该模型是使用 c 语言描述的一个高级的参考模型, 可以实现与 AES DUT 一样的功能, 用激励 AES DUT 的相同激励去驱动 AES C 模型, 便可以得到期望的结果, 最后在比较器中, 将期望的结果和在 AES DUT 中采样得到的结果做比较, 判断该验证场景是否通过。

AES Testcase Library 中包含了用户编写的测试用例(Testcae), 这些测试用例可以调用 AES_sequencer 中对应的序列对 AES 数据项目做随机约束, 从而得到期望激励。还可以根据后续的需求添加扩充测试用例库的用例, 目前用例库中编写了 8 个测试用例, 如表 1 所示。

每个 AES 通道都有各自的 AES 数据项目去驱动, 在 AES 数据项目中定义了需要激励的输入变量, 这些变量如表 2 所示。

AES_driver 信息驱动与采样一个通道的加密时序如图 6 所示所示。驱动 AES 模块时, 首先需要通过 AES_driver 对 AES 做基本的配置。

表 1 AES 测试用例库列表

测试用例名称	描述
aes_128_key_len_enc_tc	测试 aes key length 为 128 比特时的加密场景
aes_256_key_len_enc_tc	测试 aes key length 为 256 比特时的加密场景
aes_128_key_len_dec_tc	测试 aes key length 为 128 比特时的解密场景
aes_256_key_len_dec_tc	测试 aes key length 为 256 比特时的解密场景
aes_multi_channel_enc_tc	测试多个 aes channel 同时加密的工作的场景
aes_ecb_mode_tc	测试 aes 在 ecb 工作模式下的场景
aes_xts_mode_tc	测试 aes 在 xts 工作模式下的场景
aes_lpa_mode_tc	测试 aes 在 lpa 工作模式下的场景

表 2 AES 数据项目列表

变量名称	描述
data_in	加密和解密前的输入数据, 该其为一个宽度为 128 bit, 深度为 1028 的数组
key1	宽度可变的第一密钥
key2	宽度可变的第二密钥
hash_key	对第一个第二密钥进行加密的密钥
mode	aes 正常模式下的工作模式, 包括 xts 和 ecb 模式
dec_enc_mode	选择 aes 是工作在加密模式还是解密模式
unit_sz	一个数据单元的长度
non_main_mode	选择 aes 是工作在正常模式还是特殊的 lpa 模式
cts_en	cts 解密使能
transmit_delay	数据传输延时

配置步骤如下: (1) 通过 key_length_128 和 key_length_256 选择加密的密钥长度是 128 比特还是 256 比特。(2) 控制 mode_in_xts 和 mode_in_ecb 信号选择 aes 是工作在 xts 模式还是 ecb 模式。(3) 驱动 hash_key_av 为高电平时, 输入 hash_key 的值。(4) 驱动 key1_av 和 key2_av 为高电平时, 输入 key1 和 key2 的值。(5) encrypt 和 decrypt 信号选择是进行加密还是解密模式。(6) 输入 transfer_size_in_beats 确定一个数据单元的大小。在配置完 aes 的基本信息以后, 向 AES 输入待加密

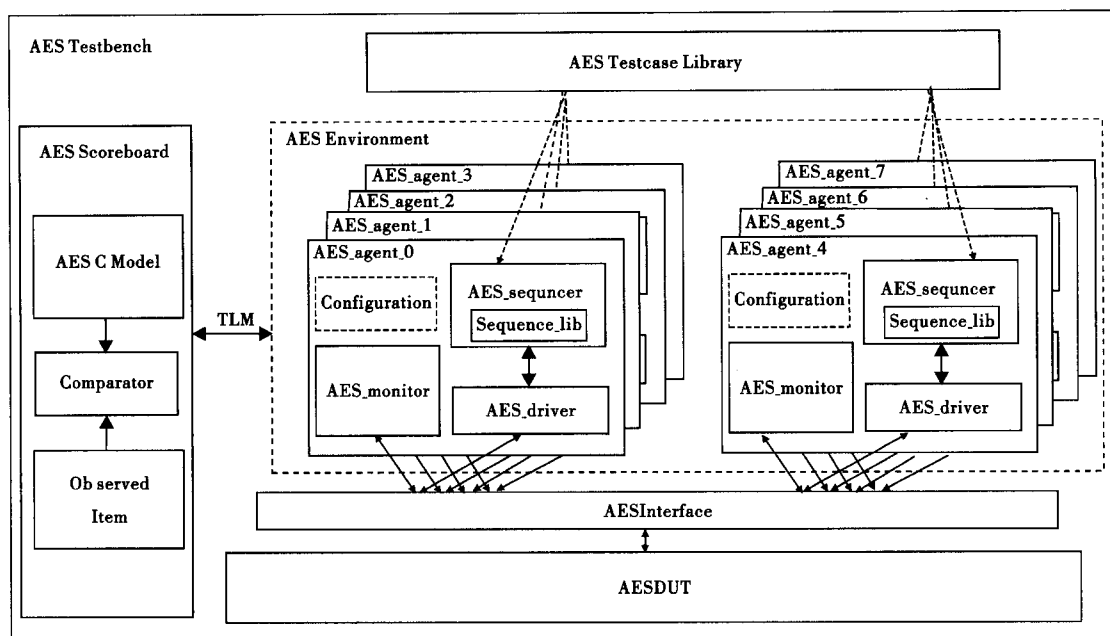


图 5 基于 UVM 的 AES 验证平台

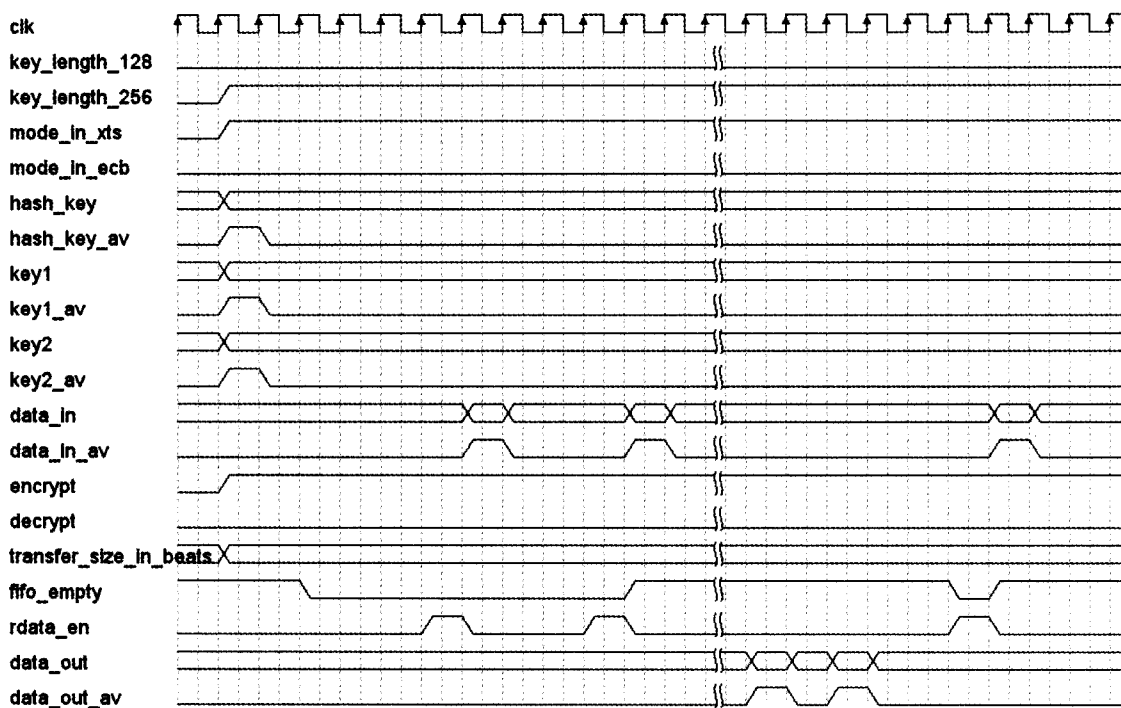


图 6 AES 驱动与采样时序

数据,只有当 fifo_empty 信号为低电平且 rdata_en 输出高电平脉冲时,可将 AES 的 data_in_av 信号拉高,同时给 data_in 信号赋值。

采样 AES 模块时,分为两部分采样 AES 的信息,一是 AES 模块的输入信号信息,二是 AES 模块的输出信号信息。当数据单元相关的传输信息采集完以后,AES_monitor 会通过传输模型将采样信息

传输给 AES_scoreboard。采样的输入信息用于驱动在 AES_scoreboard 中的 AES C 语言模型,采样的输出信息用于在 AES_scoreboard 中做采样信息的一致性比较。

在 AES_scoreboard 中主要由 AES C 模型,AES C 模型的驱动模块与监控模块,比较器三部分组成。首先 AES_scoreboard 将接收到的 AES_mo-

nitor 传输过来的输入采样信息给 AES C 模型的驱动模块,该驱动模块会将输入采样信息解析成 AES C 模型能识别的数据类型,然后按照 AES C 模型的输入要求对其进行驱动,AES C 模型的监控模块会采样 AES C 模型的输出信息并将其打包传输给比较器,比较器接受 AES 的输出信息和 AES C 模型的输出信息,按照一个数据单元的信息长度对相关的命令与数据作比较,从而判断此次验证场景的正确性,若正确则打印 pass,否则打印 failed.

AES 模块的解密步骤是机密的一个逆过程,只需按照 AES 解密的协议标准和时序驱动、采样和比对即可.

4.3 验证结果分析

以 aes_multi_channel_enc_tc 测试用例为例分析仿真结果.此测试用例的验证场景是 AES 模块多个通道同时进行数据加密,密钥长度(128 比特或是 256 比特)、工作模式(xts 模式或 ecb 模式)、数据单元长度、待加密数据、密钥均为随机约束得到,AES_driver 使用这些数据项目驱动 AES DUT,AES_monitor 采样 AES DUT 的输入输出信息,并将其转化打包.ASE_monitor 采样得到的一个通道的数据项目可以看到该通道工作的信息,该通道加密密钥的长度为 256 比特,工作 ecb 模式,数据单元的大小为 4 kB,传输延时为 0,cts 功能禁止,还可以看到每笔待加密数据和其对应的加密后数据.

可以看到,此测试用例 aes_multi_channel_enc_tc 比对成功.在此次仿真过程中一共打印了 1 040 条仿真信息,没有警告、一般错误或严重错误信息,在 rsnst, test_done, aes_driver, aes_monitor, aes_scoreboard 模块中分别打印的信息数量也在报告中给出了.若测试用例失败,这些打印信息便是至关重要的调试参考信息.

5 结束语

在验证领域,验证语言的整齐划一、仿真平台的统一、发展正规高效的验证方法学,一直是 IC 验证的发展趋势^[6].UVM 验证方法学吸收了当前诸多主流验证方法学的优点,并且获得了如 Cadence、Synopsys 和 Mentor 等 EDA 公司的仿真软件支持,它的高效、高可重用化、高度自动化、开源化已经得到了很多工程师们的肯定.

参考文献:

- [1] 李磊,罗胜钦.基于 VMM 方法的 SOC 集成验证[J].电子测量技术,2011(1):1
- [2] Announcing the Advanced Encryption Standard[S].美国空军用标准:FZPS-PVB-197 Federal Information Processing Standards Publication. 2001.
- [3] Accdlera. Universal verification methodology 1.1 user's guide[M]. Cadence Design Systems Inc., Mentor Graphics Corp., Synopsys Inc., 2011,5: 2
- [4] Accdlera. Universal verification methodology 1.1 class reference[M]. Cadence Design Systems Inc., Mentor Graphics Corp., Synopsys Inc., 2011,6: 342
- [5] Sharon Rosenberg. A practical guide to adopting the universal verification methodology [M]. Cadence Design Systems Inc., 2010,5: 9
- [6] Chris Spear. System Verilog for Verification [M]. Synopsys Inc., 2008: 5

作者简介:

王小力 男,(1956-),教授,博士生导师.研究方向为高性能 VLSI 与优化设计、集成化芯片系统设计与基础研究、光纤通讯与光波分复用(WDM)技术.

田 劲 男,(1985-),硕士研究生.研究方向为 SSD 固态硬盘主控芯片的设计与验证.

(上接第 85 页)

- [6] 杜华. Linux 编程技术详解 [M]. 北京:人民邮电出版社. 2007:280-281.
- [7] 周立功. ARM 嵌入式 MiniGUI 初步与应用开发范例 [M]. 北京:北京航空航天大学,2006:25-26.
- [8] 李广丽,刘遵雄,张宏斌. 肿瘤图像病理诊断系统的设计[J]. 华东交通大学学报,2007,24(5):99.

作者简介:

甘 岚 女(1964-),硕士,教授.研究方向为模式识别与图像处理.

龚礼武 男,(1985-),硕士研究生.研究方向为嵌入式系统与应用.