Robust Functional Verification Framework Based in UVM Applied to an AES Encryption Module

Title	Robust Functional Verification Framework Based in UVM Applied to an AES Encryption Module
Publication Type	Conference Paper
Year of Publication	2018
Authors	Plasencia-Balabarca, F., Mitacc-Meza, E., Raffo-Jara, M., Silva-Cárdenas, C.
Conference Name	2018 New Generation of CAS (NGCAS)
ISBN Number	978-1-5386-7681-3
Keywords	AES encryption module, compositionality, cryptography, design requirements, digital design industry, direct verification methodologies, Encryption, formal verification, functional verification, hardware description languages, high-level designs, Industries, information-security applications, Measurement, Metrics, pubcrawl, Reliability engineering, resilience, Resiliency, robust functional verification framework, Scalability, scalable verification, Standards, System Verilog-based functional verification, Universal Verification Methodology, UVM, Verification Framework

Abstract

This Since the past century, the digital design industry has performed an outstanding role in the development of electronics. Hence, a great variety of designs are developed daily, these designs must be submitted to high standards of verification in order to ensure the 100% of reliability and the achievement of all design requirements. The Universal Verification Methodology (UVM) is the current standard at the industry for the verification process due to its reusability, scalability, time-efficiency and feasibility of handling high-level designs. This research proposes a functional verification framework using UVM for an AES encryption module based on a very detailed and robust verification plan. This document describes the complete verification process as done in the industry for a popular module used in information-security applications in the field of cryptography, defining the basis for future projects. The overall results show the achievement of the high verification standards required in industry applications and highlight the advantages of UVM against System Verilog-based functional verification and direct verification methodologies previously developed for the AES module.

URL https://ieeexplore.ieee.org/document/8572292
DOI 10.1109/NGCAS.2018.8572292
Citation Key plasencia-balabarca_robust_2018

AES encryption module Compositionality Cryptography design requirements digital design industry direct verification methodologies encryption formal verification functional verification hardware description languages high-level designs Industries information-security applications Measurement Metrics pubcrawl Reliability engineering resilience Resiliency robust functional verification framework Scalability scalable verification standards System Verilog-based functional verification Universal Verification Methodology UVM Verification Framework