Indian Patent Advanced Search System

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

Patent Search

Invention Title	DESIGN SPACE EXPLORATION OF AN OPTIMIZED HARDWARE TROJAN DETECTABLE/SECURED DATAPATH DURING HIGH LEVEL SYNTHESIS
Publication Number	23/2015
Publication Date	05/06/2015
Publication Type	INA
Application Number	1666/MUM/2015
Application Filing Date	24/04/2015
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F15/16

Inventor

Name	Address	Country	Nationality
SENGUPTA, Anirban	Indian Institute of Technology, Indore, PACL Campus, Near Veterinary College, Survey No. 113/2-B, Mhow, MP, India, PIN: 453441	India	India

Applicant

Name	Address	Country	Nationality
INDIAN INSTITUTE OF TECHNOLOGY, INDORE	Indian Institute of Technology, Indore, PACL Campus, Near Veterinary College, Survey No. 113/2-B, Mhow, MP, India, PIN: 453441 and also having a place of business at IET DAVV Campus, M Block, Khandwa Road, Indore, MP, India, PIN: 452017	India	India

Abstract:

An evolutionary algorithm (EA) driven novel design space exploration (DSE) of an optimized hardware Trojan secured datapath based on user power-delay constraint during high level synthesis (HLS) is presented. The present invention provides DSE for hardware Trojan detection includes a problem encoding technique that enables exploration of efficient distinct vendor allocation as well as enables exploration of an optimized Trojan secured datapath structure. The exploration backbone for the present invention is bacterial foraging optimization algorithm (BFOA) which is known for its adaptive feature (tumbling/swimming) and simplified model. Results of comparison with recent approach indicated an average improvement in quality of results (QoR) of >14.1%

Complete Specification

CLIAMS:1. A method to explore an optimized hardware Trojan secured dual/ double modular redundant (DMR) scheduled data flow graph (datapath system) design, during high level synthesis by detecting hardware Trojan in at least one hardware operator inserted by an third party intellectual property (3PIP) vendor/adversary, by a system, said method comprising:
receiving, by a receiving module:
at least one of a module library pre-stored or generated;
one or more control parameters;
a behavioral description of one or more control data flow graph comprising at least one operation and a (associated) dependency information of said operation; and one or more predefined user parametric constraints associated with area/ power and time execution/delay;
exploring, by means of one or more pre-stored design space exploration mechanism in a resource configuration exploration module, one or more new resource configurations (Rn), based on said control parameters received and said behavioral description; wherein
generating, using resource configuration exploration module, a new design solution (Rx) by encoding said new resource configurations (Rn) explored and distinct vendor assignment procedure (AV); thereby
building, using a Trojan detection module, one or more dual/ double modular redundant (DMR) scheduled data flow graph comprising one or more schedule of an original unit and one or more schedule of a duplicate unit based on said design solution (Rx) generated;
allocating, using the Trojan detection module, operations from said DMR scheduled data flow graph built to one or more hardware operator, wherein said hardware

View Application Status