Oral S05

Advanced Synthesis, Reliability and Security Techniques

Date/Time 8/3 (三) 14:30-15:30

Chair(s) 謝東佑教授 / 國立中山大學電機工程學系
温宏斌教授 / 國立陽明交通大學電機工程學系

S05.1 14:30 – 14:42

On Efficient Modeling and Test Generation of Hard-to-Detect Combinational Hardware Trojans

Tong-Yu Hsieh, Hsin-Hsien Lin, and Jun-Tsung Wu
Department of Electrical Engineering, National Sun Yat-sen University

In the context of hardware security, it is crucial to identify the most likely suspects of hardware Trojans in a target circuit. In the literature, this issue has also been widely investigated by targeting various types of hardware Trojans. In this paper, combinational hardware Trojans are considered and a much more efficient methodology is proposed to model Hard-To-Detect (HTD) hardware Trojans that are more hardware-security risky. The experimental results show that the proposed modeling methodology reduces 96.44% hardware Trojans, while that for the previous work is 70.84%. This allows us to put more focus on the riskiest lines where hardware Trojans may be implanted. The other major contribution of this work is that we also develop an efficient test generation methodology that can generate compact test patterns capable of detecting these identified HTD Trojans. In addition to aiming to detect as many HTD Trojans as possible, we also include a particular compression process in our pattern generation methodology in order to minimize the number of the generated test patterns. The experimental results show that the test pattern size is reduced by 84.48% when compared to the previous work. Also, the generated test patterns achieve 97.08% detection coverage of HTD Trojans.

S05.2 14:42 – 14:52

Enhancing ILP-based Identification of Rational-Weight Threshold Logic Gates

Ting-Yu Yeh[1], Yueh Cho[1], Yung-Chih Chen[1], and Wang-Dauh Tseng[2]
[1]Dept. of Electrical Engineering, National Taiwan University of Science and Technology
[2]Dept. of Computer Science and Engineering, Yuan Ze University

In CMOS-based current mode realization, the threshold logic gate (TLG) implementation with rational weights has been shown to be more cost-effective than the conventional TLG implementation without rational weights. The existing method for the rational-weight TLG identification is an integer linear programming (ILP)-based method, which could suffer from inefficiency for a Boolean function with a large number of inputs. This paper presents a two-stage method to enhance the ILP-based method. In the first stage, we propose some rules to directly transform the given conventional TLG into a rational-weight TLG. If the transformation does not reduce the implementation cost, we then conduct the second stage, in which we perform the ILP-based method with a simplified formulation to optimize the

rational-weight TLG. We conducted the experiments on a set of TLGs with 4 ~ 15 inputs. The results show that the proposed method has a competitive quality with an average ratio of 0.92, compared to the ILP-based method. Additionally, the proposed method spent only an average of approximately 21% of CPU time.

S05.3 14:52 — 15:02

A TMR Based Error-Tolerant Memory Protection Scheme without Additional Storage for Machine Learning Applications

Tong-Yu Hsieh, Yu-Ren Chiu, and Wei-Ji Chao
Department of Electrical Engineering, National Sun Yat-sen University

In this paper, a TMR (Triple Modular Redundancy)-based protection scheme for memories for machine learning applications is proposed. In particular, no additional storage is required to store the needed data copies, and thus the incurred cost can be greatly reduced. A pedestrian detection machine learning model is also employed as a case study. Our proposed scheme well exploits the inherent machine error-tolerability of AI machine learning models. A detailed error-tolerability analysis process is carried out. Accordingly, the non-critical memory bits that have negligible impacts on the machine detection results are identified and used to store the data copies of TMR for protecting the critical bits. Possible protecting models for critical bits based on the proposed scheme are then developed and discussed, together with their hardware implementation. The experimental results show that our scheme achieves effective memory protection with only negligible cost.

S05.4 15:02 — 15:12

Diagnosing Double Faulty Chains through Failing Bit Separation

Cheng-Sian Kuo[1], Bing-Han Hsieh[1], James Chien-Mo Li[1], Chris Nigh[2], Gaurav Bhargava[2], and Mason Chern[3]
[1]Department of Electrical Engineering, GIEE, National Taiwan University
[2]Qualcomm Technologies, Inc.
[3]Qualcomm Semiconductor Limited

Diagnosing scan chain faults plays a key role in ramping up production yield. High test compression ratios of modern designs increase the challenge of scan chain diagnosis. We propose a technique to address this problem through separating the superpositioned chain fault effects to diagnose chips with two faulty scan chains. Experiments are conducted on both simulated and silicon test data, and the proposed method showed improvements over commercial tools in resolution (2.38) and accuracy (92.0%). We did find failing chips that potentially have a systematic problem in the same double chains.

S05.5 15:12 — 15:22

Compiler of Reed-Solomon Error Correction Codec for IEEE Std 802.3bs Supporting a Very High Throughput of 400 Gbps

Lin Liu[1], Chi Lai[1], Shi-Yu Huang[1], and Ka-Yi Yeh[2]
[1]Department of Electrical Engineering, National Tsing Hua University
[2]Industrial Technology Research Institute

Error Correction is often indispensable in a modern digital communication system that transmits data at a very high speed. Recently published IEEE Std 802.3bs requires an astounding throughput of 200Gbps or even 400Gbps while using the Reed-Solomon Code (RS-Code) for Error Correction to protect the integrity of the transmitted data. An RS-Codec supporting such a high throughput demands sophisticated hardware implementation. In this paper, we present a Reed-Solomon Codec complier that makes contributions in two aspects. First, our parameterized Codec satisfying IEEE Std 802.3bs using RS(544, 514), in which the throughput can be boosted on demand by setting some "configuration". Second, our RS-Codec can easily produce an area and power efficient RS-Codec design satisfying a target throughput in just minutes while supporting easy process migration. Experimental results using 28nm and 90nm CMOS processes are presented to demonstrate its effectiveness.

S05.6 15:22 — 15:32

Multi-level Exploration for Single-Event Double-Node Upsets (SEDU) in Sub-65nm Radiation-Hardened Latches

Sam M.-H. Hsiao, Lowry P.-T. Wang, Ralf E.-H. Yee, and Charles H.-P. Wen
ECE Department, National Yang Ming Chiao Tung University

A single-event double-node upset (SEDU) may appear to result in an erroneous state of the storage element due to the scalability of transistor features. Therefore, SEDU must be well addressed from the perspective of circuit reliability, especially for safety-critical electronics. To better understand the technology scaling impact, we re-examine SEDU in different advanced technologies (including 7-nm finFET, 45-nm bulk CMOS, and 65-nm bulk CMOS). An integrated multi-level framework is developed with the current-source modeling derived from the device-level TCAD simulation, combined with voltage calculation derived from the circuit-level SPICE simulation.

To adequately capture the probability of errors occurring in the latch design under all possible scenarios, this paper also considers a variety of environmental factors, such as striking angles and technology nodes. Additionally, three classical latch designs (i.e., TMR, DICE, and HLR) have been implemented in different technologies and are well-calibrated for experiments. According to experiment results, it is evident that SEDU is highly dependent on both the physical layout of the design as well as its design style. DICE is found to be the most susceptible to SEDU in all three manufacturing technologies, whereas TMR and HLR can be immune to SEDU in the 45-nm and 65-nm technologies due to a lack of sufficient charge to upset more than two nodes. It is, therefore, essential to consider both the physical layout and the manufacturing technology employed for ensuring the robustness of a radiation-hardened design against particle strikes.