The Logic Function Extraction Technology Based on Automatic Correction Algorithm

Da Xiao & Jinlong Fei & Yuefei Zhu & Shengli Liu & Zhaolin Zhang
Computer network department, ZhengZhou Information Science University, ZhengZhou, HeNan, China

ABSTRACT: Proposed equivalent item extraction based on contradictory truth table logic function algorithm, gives details of the algorithm implementation process. Select the one with eight inputs, two outputs of the chip to work waveform genera Test. Test results show waveforms attribute recognition model designed in this paper correctly identified the properties of the seven pins, re-use automatic correction algorithm, the successful implementation of misidentification pin Correction properties, complete all ten waveforms attribute recognition.
KEYWORD: logic function extraction; attribute identification; algorithm; self-correction

1 INTRODUCTION

In recent years, for better improving the using safety of hardware chip and electronic equipment, the work aiming at the detection of hardware Trojans has drawn more and more attention and has formed many different detection schemes of hardware Trojans. There is a representative which is based on the analysis of the bypass presented by Wang Liwei, Luo Hongwei, Yao Ruohe, et al. They detected hardware Trojans in chip by using the singular value decomposition algorithm for statistical processing though the power consumption analysis of transient changes. Though the test of the simulation experiment, they detected the hardware Trojans which was 2 orders of magnitude smaller than the original circuit successfully[1]. Wang Liwei, JiaKunpeng, et al. also proposed a non-destructive detection method of hardware Trojans which was based on Mahalanobis distance and accomplished the test of hardware Trojans in AES circuit[2]. Aiming at the model of hardware Trojans power consumption having been established, Liu Changlong, Zhao Yi, et al. realized the hardware Trojans' detection by analyzing the characteristics and rules of correlation coefficient, optimizing the detection coefficient and using the interval overlap ratio. The experimental result showed their testing method can increase the robustness over one time[3]. Gao Hongbo analyzed the instruction-triggered hardware Trojans deeply, raised its graph, used the mind of model testing, designed hardware Trojans detection algorithm and detailed implementation process and verified the possibility of the model and the algorithm through the example. By the absolute information divergence index of the projection pursuit technique[4]. Zhang Peng, Wang Xingcheng et al. transformed the high dimensional bypass signal in logical chip movement into a low dimensional subspace and on the basis of this they analyzed the signal characteristic having been conversion as the basis of Trojans ' detection, and verified it by AES-128 Trojans circuit[5]. Liu Huafeng analyzed hardware Trojans' detection and the method of the testing which based on FPGA deeply, comprised and analyzed the representation, classification and conventional detection method of the hardware Trojans. Based on this, he designed the combinational hardware Trojans circuit and time sequence hardware Trojans circuit, and he built the experiment platform, tested it and verified the possibility of the hardware Trojans' detection.[6] In foreign countries, there are many related literatures of the hardware Trojans' detection[7] [8].

To be able to quickly and effectively target hardware Trojan detection logic chips, a feasible method is based on a logical feature comparison method to detect the target logic chip with expectations Design or logic functions described are the same. If they are consistent, it is determined that the target is not a hardware logic chip trojan, otherwise the logic determines that the target function of the chip design and the expected Inconsistent, finds its interior contains a hardware Trojan. This paper would focus on how to solve the error in the chip pin attribute recognition when the

logic function equivalence has been extracted.

2 THE DESIGN OF EXTRACTION ALGORITHM

Self-Correcting Algorithm of Waveform Property Based on the Contradictory Truth Table

According to this paper, based on the analysis of the waveform attributes contradictory truth table of the automatic correction and research findings, the paper design automatic correction waveform properties based algorithm flow contradictory truth table shown in Figure1.

Because the ultimate purpose of the algorithm is to generate a truth table at the time, and be able to assist, adjustments and amendments, according to some contradictory truth table truth table entries generated in the process of working waveform attributes appear before this recognition results ultimately achieve the correction of recognition results waveforms property. Therefore, when implementing the algorithm, the first wave properties extracted from the results of the work identified in the results identified before, and as a basis, the operating waveforms into two attribute sets, and each element of the collection numbering, i.e. for the set of waveforms is divided into $I_1, I_2, \cdots, I_m$, On the elements of the collection to be prepared for the, $O_2, \cdots\cdots, O_n$ In each element of the collection in fact corresponds to the target chip in a pin number, so the fact that the work is to identify the waveform identification of the target chip pin attribute features.

Later it will scan all the waveforms of the set from the present time to locate the nearest one jump, long jump that occurs in the entire collection of attributes of the waveforms can be any one. After this jump as a reference to extract the set of all the digital waveforms, and all values in the set operation waveform after this transition occurs before the transition, which will form a truth table entry value. Note that when extracting the value, there is a certain response delay due to the chip, and therefore to extract the set of input data should be extracted before the transition time. Extracting the data in the collection should be after the time to extract the transition, i.e., in consideration of the delay on the basis of the chip to ensure that the extracted data is true the input data and the output data after the chip stable otherwise extracted the truth table for the data to be wrong.

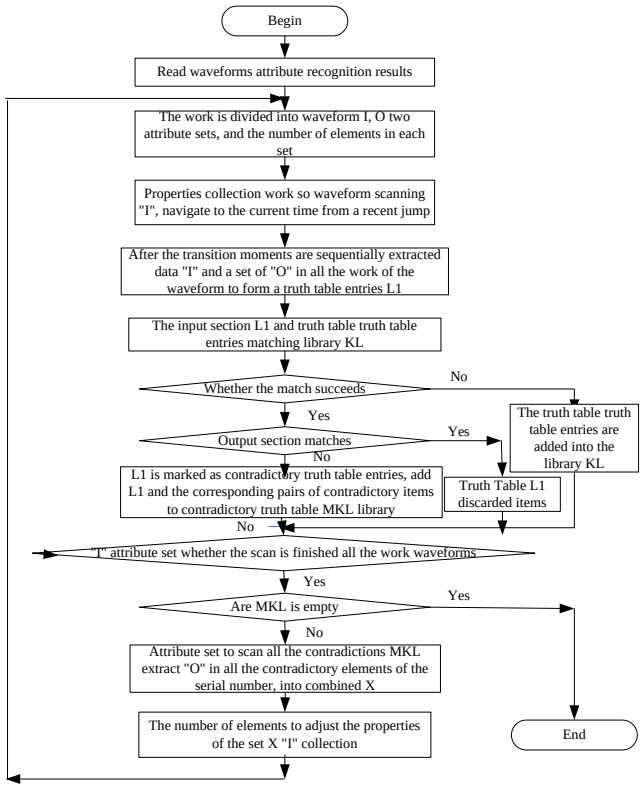

Figure1: Based on the work of the waveform properties contradictory truth table entries automatically correct algorithm

Extract the truth table for the new library and historical truth table entries stored match. If the current collection to the new item appears in the truth table truth table library, check the current output section of the library truth table truth table entry corresponding to the truth table entries in the output section is the same, if the same is shown to be a truth table entry already exists without adding. If the truth table of the truth table, and the library entry do not match, it indicates that this is a truth table for the new record is to be added to the library in the truth table. If the output of a partial match is unsuccessful, then the truth table currently collected and the true value of the library in terms of a truth table entries mutually contradictory, this time will be marked as contradictory truth table entries, and add true value to the conflict table library collection. Continue to work after the set to scan the input waveform, if the scan is not the end, then continue next scan until you find the current time from the nearest next jump, followed by the extraction process and have the same truth table entry process.

If the entire set of input waveforms all scanned, then checking whether the collection is empty, the collection is empty indicated that no contradictory truth table entry, the algorithm process ends.

If the detected conflicting truth table entry is found, extract all contradictions number of items in MK_L truth table, sign the serial number belongs to the O set of all elements for reproduction of the contradictions, and these sets corresponding waveforms property adjustments that might be the

work of these waveforms waveform I set, and will adjust the waveform to I set to work, and then re-scan and extract the true value. This constant cycle until the truth table entries generated when the true value of its contradictions library MK_L record is empty.

In this way eventually able to use the process to extract the truth table that appears contradictory truth table entries, automatically correcting the work waveform attributes such property in accordance with the work of the waveform to extract the truth table after correction does not appear contradictory truth table entries, finally finish the extraction of the truth table entries.

3 TESTING AND ANALYSIS

3.1 *Functionally equivalent extraction process of single logic chip*

To test this design feasibility equivalent logic chips feature extraction methods, we designed an 8 input / 2 output of combinational logic chips, in accordance with the process we design logic chip equivalent function to extract the program, carried out a detailed test. Some of the main test results are shown in Table 1 and Table 2.

Table 1 reflects the logic chip pin attribute recognition results, we can see from Table 1, during recognition, since it is difficult to identify the model parameters set exactly match the real circuit model, so there is some false positives phenomenon. That is, the vast majority of pin waveforms satisfy both the "input" transition properties, but also have to meet the "output" transition attribute. Since the logic chip pin attribute identifies the problem of this study is that only one-way analysis of pin properties, therefore, meet the ratio "input" and "output" attribute is identified based on the work of the waveform. Selection attribute as a higher ratio of the determination result of the working of the waveform.

Table 1 Pin attribute identifies the result of the logic chips

Pin No.	Pin Properties	The number of transitions meet the "input"	The number of transitions meet the "output"	Recognition results
P1	input	8594	29	input
P2	input	7942	0	input
P3	input	3948	9854	output
P4	input	6048	15340	output
P5	input	13849	583	input
P6	input	2975	6865	output
P7	input	8931	0	Input
P8	input	13946	0	input
P9	output	486	7952	output
P10	output	0	8945	output

During the pin attribute recognition process, setting recognition model parameter incorrectly and the identification process carried out by the ratio of the properties identified will result in the target chip waveforms attribute recognition errors, these errors may cause conflicts occur when extracting the truth table items. After statistics showed that the chip waveforms attribute recognition results given in Table 1, in the extraction of the truth table, produced a total of 139 groups contradictory truth table entries. Select from 3 groups of representative contradictory truth table entry, as shown in Table 2.

Contradictory truth table does not just include the items in Table 2, but on the table by the contradictions true value marked items have been able to fully recognize the contradiction pin number. Contradictory pin number in table is the misjudgment pin $P3, P4, P6$ in Table1. The contradictions of the pin from the output to the input attribute property correction, and then work on the original waveform to extract the truth table, will no longer appear contradictory truth table entries, which can effectively reverse logic synthesis, implement logic functions equivalent to extract.

Table 2 Typical appear contradictory truth table to extract the truth table entries

input	output	Contradictory pin numbers
10110	10110	O_1, O_3
10110	00110	
10110	10010	
01101	01111	O_1, O_2
01101	00111	
01101	10111	
10101	01001	O_1, O_2, O_3
10101	01101	
10101	11101	
10101	10001	

4 ACKNOWLEDGMENT

This work is supported by the National Science-Technology Support Plan Project of China (No. 2012BAH47B01), by the Natural Science Foundation of China (No. 61309007), and by the Municipal Science and Technology Innovation Team Project of Zhengzhou (No. 10CXTD150).

5 SUMMARY

Through analyzing the logic chip waveforms, extract its equivalent logic function is an effective way to achieve hardware Trojan detection. Design Contradictory truth table based on the work of self-correction algorithm waveform attributes can solve

this problem, be able to provide direct support for hardware Trojan detection.

REFERENCES

[1] Wang Li-Wei,Luo Hong-Wei,YaoRuo-He. Side-channel analysis-based detection approach of hardware Trojans. Journal of South China University of Technology (Natural Science Edition), 2012, Vol.40 (6):1-10.

[2] Wang Li-Wei,Jia Kun-Peng,Fang Wen-Xiao,Dong Qian. An approach to detecting hardware trojans based on mahalanobis distance. Microelectronics, 2013, Vol.43 (6):817-820.

[3] Liu Chang-Long,Zhao Yi-Qiang,ShiYa-Feng,FengZi-Zhu. Hardware trojan detection method based on correlation analysis. Computer Engineering, 2013, Vol.39 (9):183-185,195.

[4] Zhang Peng,ZouCheng,Deng Gao-Ming,Chen Kai-Yan. A hardware trojans design using the correlation analysis of electromagnetic emanation. Journal of Huazhong University of Science and Technology (Natural Science Edition), 2010, Vol.38 (10):22-25(in Chinese)

[5] Liu Hua-Feng. Design and detection of hardware trojan horse based on FPGA. Guangzhou, China: South China University of Technology.2011.

[6] R. Rad, J. Plusquellic and M. Tehranipoor. Sensitivity snalysis to hardware trojans using power supply transient signals. In Proc. of Workshop on Hardware -- Oriented Security and Trust 2008, pp 3–7

[7] Alexander Adamov, Alexander Saprykin, DmitriyMelnik, Olga Lukashenko.The problem of hardware trojans detection in system-on-chip. CAD Systems in Microelectronics, 2009.CADSM 2009.10th International Conference -- The Experience of Designing and Application of, 24-28 Feb.2009: (Lviv-Polyana), P178-179

[8] Gao Hong-Bo. Research on detection techniques of instruction -- triggered hardware trojanhorse. Zhengzhou, China: PLA Information Engineering University, 2013.