A Novel Hardware Trojan Detection with Chip ID Based on Relative Time Delays

Yijun Yang, Liji Wu*, Xiangmin Zhang, Jianben He

Institute of Microelectronics, Tsinghua University, Beijing 100084, China yangyj16@mails.tsinghua.edu.cn; lijiwu@mail.tsinghua.edu.cn; zhxm@mail.tsinghua.edu.cn; jessiehe@hust.edu.cn

***Abstract*—This paper introduces a hardware Trojan detection method using Chip ID which is generated by Relative Time-Delays (RTD) of sensor chains and the effectiveness of RTD is verified by post-layout simulations. The rank of time-delays of the sensor chains would be changed in Trojan-inserted chip. RTD is an accurate approach targeting to all kinds of Trojans, since it is based on the RELATIVE relationship between the time-delays rather than the absolute values, which are hard to be measured and will change with the fabricate process. RTD needs no golden chip, because the RELATIVE values would not change in most situations. Thus the genuine ID can be generated by simulator. The sensor chains can be inserted into a layout utilizing unused spaces, so RTD is a low-cost solution. A Trojan with 4x minimum NMOS is placed in different places of the chip. The behavior of the chip is obtained by using transient based post-layout simulation. All the Trojans are detected AND located, thus the effectiveness of RTD is verified.**

Keywords- hardware Trojan; chip ID; sensor chain; time-delay; side-channel signal

I. INTRODUCTION

The integrated circuit (IC) foundries are now wilder-distributed. As the perplexity of third-party companies and vendors involved increased, hardware security is facing more serious safety threats from various malicious attacks and modifications (the so-called Hardware Trojans). A Trojan is usually inserted into a very small part of the circuit and only very rare events and conditions can trigger it, thus, it is almost impossible to find it out during functional or ATPG testing process[1].

Most existing detect methods can be classified into two categories: Trojan activation and side-channel signal analysis [2-4], and the latter can be further distinguished between power parameter measurement and time-delay measurement[2].The Trojan activation needs to fully activate the Trojan which is usually difficult to achieve for the innumerable realistic states.While for the second approach, the partial activation is still needed and the biggest challenge is the measurement precision affected by unavoidable process variations and noise [2].

To do some improvement about the existing detect method implementing power supply signals analysis, Reza, Jim and Mohammad in 2008 proposed a modified idea which detects anomalies by setting multiple supply ports combined with calibration technique [5]. Later in 2011, a RON Network [2] is put forward to mitigate the deviation caused by environmental and process variables. The technique proposed in [6] has similar idea, but it uses sensor as the monitor. To further get rid of the process variation problem, a variation model on a lot level [7] is proposed in 2016.

Time-delay analysis, serving as an easily-monitored index, is being readily employed. A "clock sweeping technique" [3] is proposed whose advantage is no additional hardware compared with existing delay-based Trojan detection methods. This technique collects delay information from both critical and noncritical paths and generates signatures indicating whether there is any Trojan. Yuan Cao and his colleagues proposed converting the current activity to time interval [10], thus achieving Trojan detection by time-delay analysis. Another methodology has been put forward to establish a series of fingerprints as a comparison standard, and this strategy is particularly effective for explicit payload Trojans but not for implicit ones [8-9].

Our Contribution. In this paper, the theory of RTD is introduced, and the effectiveness of RTD is verified by post-layout simulations.

We distribute two groups of sensor chains to a chip which is suspected Trojan-inserted. Every sensor chain owns its specific number. The sensor chains consist of drivers, and interconnection wires, and both of them could monitor parasitic resistance and parasitic capacitance caused by the chip, which result in the time-delay of each sensor chain. Each sensor chain has different location and is adjacent to various components, so every chain's time-delay differs from each other. We put these time-delays by the ascending order, and get a sequence consisted of the numbers of sensor chains. This sequence is just the chip ID. Each chip due to its special structure, scale and sensor chains distribution, has a unique sequence of the serial numbers of sensor chains. Once a chip is Trojan-inserted, its ID would be changed. So the Trojan can be detected by identifying the ID of the chip. The time-delays can be obtained by the transient simulation, and the genuine ID of the chip is a relative value. Therefore RTD does not need any golden chip. Moreover, the inverter chains can be distributed in the layout level utilizing the free space of the chip, which means almost zero area overhead.

978-1-5386-0533-2/17/$31.00 ©2017 IEEE

Authorized licensed use limited to: Hong Kong University of Science and Technology. Downloaded on May 23,2023 at 02:25:44 UTC from IEEE Xplore. Restrictions apply.

The rest of this paper is organized as follows. Section II introduces the background including the time-delay of inverter and interconnection wire. Section III introduces the RTD detection method in detail. Section IV describes four experiments and analyzes the results. Finally, Section V concludes this paper.

II. BACKGROUND

In this section, we will introduce the structure of sensor chain, then we will formulate the time-delay generated by the driver such as inverter. Finally, we will describe the interconnection wire model and its time-delay.

A. Time-delay Principle Analysis of sensor chain

As the basic unit of hardware Trojan detection circuit, the sensor chain can be abstracted as shown in Fig.1. The sensor chain may consist of 1) two parts, the driver and the interconnection wires, or 2) just the interconnection wires. In this paper, we choose the first structure with COMS inverter serving as the driver of the sensor chain, for its simple structure. Any other logic gate, such as NAND gate or NOR gate, could act as the driver.

Actual interconnection has parasitic capacitance as c_w, and parasitic resistance as r_w. Both r_w and c_w will be impacted by its neighboring devices on the target chip, but the devices far from them will hardly cause influence. The time-delay of the drivers will be impacted by the devices nearby because of the *Ohmic Voltage Drop* effect [11]. So, if a Trojan is inserted around a sensor chain, the time-delay of this sensor chain will increase more observably than other sensor chain, far away from the Trojan.

B. Time-delay Analysis of CMOS Inverter

As shown in Fig. 2(a), the time-delay of a CMOS inverter is decided by the time that PMOS and NMOS charge and discharge the load capacitance C_L. Switch model, as shown in Fig. 2(b), is chosen to simplify the model [11]. Citing the conclusions from [11], the time-delay of the CMOS inverter, t_p, can approximate to the (1), which is a first-order linear RC network. The time-delay of the interconnection wire is directly proportional to the product of r_w and c_w, as shown in (2).

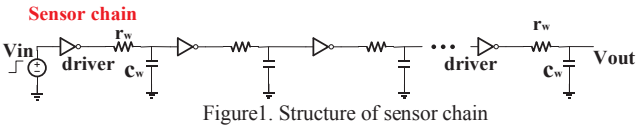
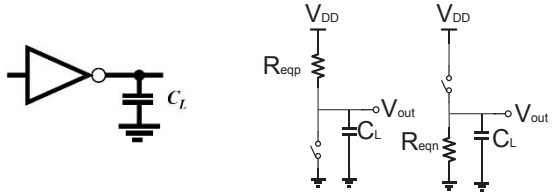
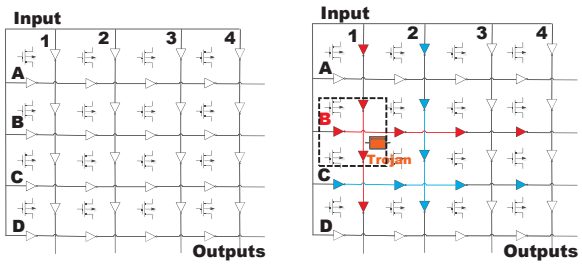


Figure1. Structure of sensor chain



(a) (b)

Figure2. Structure of CMOS Inverter. (a)Time-delay model. (b) Switch model of inverter.



(a) (b)

Figure3. Structure of hardware Trojan detection circuit

(a) Trojan-free chip. (b) Trojan-inserted chip.

$$t_{pdriver} = 0.69C_L\left(\frac{R_{eqn}+R_{eqp}}{2}\right) \quad (1)$$

$$t_{pwire} = 0.38r_w c_w \quad (2)$$

III. THEORY AND DESIGN METHOD

Fig.3(a) shows the overall structure of the hardware Trojan detection circuit. The horizontal and vertical distribution of sensor chains form a mesh topology that evenly covers the entire target chip. The horizontal sensor chains are not connected to the vertical sensor chains. The horizontal sensor chains are marked as A, B, C, D, etc. The vertical sensor chains are marked as 1, 2, 3, 4, etc.

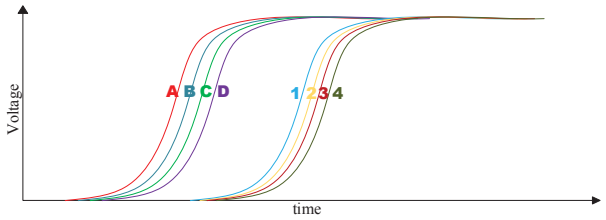
The layout of target chip is designed together with the sensor chains so that both the horizontal sensor chains and the longitudinal sensor chains will have similar but respectively varied time-delays.

By using the transient simulation function of EDA tools, one can obtain the time-delay of each sensor chain. These time-delays are naturally divided into two groups due to their different distribution directions. Arranging the time-delays in ascending order, we will get two sequences as the ID number of the target chip, for example, {A,B,C,D}{1,2,3,4},as shown in Fig. 4(a). The ID number of the chip is a relative value, which can remain unchanging in a wide range of environment variation and process deviations. Besides, we don't need to take the measurement accuracy of time-delays into account.

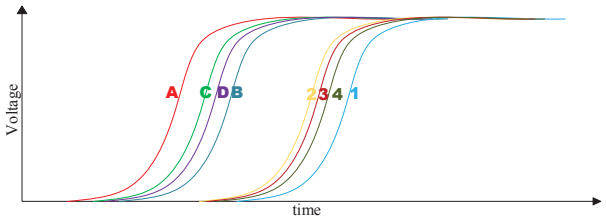
Assuming that a Trojan is inserted around the chain B and 1, which are denoted as orange in Fig.3(b), the time-delays of sensor chain B and 1 will increase significantly. In addition, sensor chain C and 2 are closer to the Trojan than other sensor chains except chain B and 1, so their time-delay will also be impacted notably.

Furthermore, the distance between the adjacent sensor chains determines the accuracy of the Trojan detection method. Therefore, the tampered ID obtained from Trojan-inserted chip could be {A,C,D,B} {2,3,4,1}, as shown in Fig.4(b). Comparing the genuine ID with the tampered ID of the target chip, one can narrow the location area of the Trojan to the dotted box inside, shown in Fig.3(b).

Authorized licensed use limited to: Hong Kong University of Science and Technology. Downloaded on May 23,2023 at 02:25:44 UTC from IEEE Xplore. Restrictions apply.



(a)



(b)

Figure 4. (a)An example time-delay sequence. (b)Changed time-delay sequence with inserted Trojan.

IV. VERIFICATION

In order to demonstrate the effectiveness of this method, we conducted four Trojan detection experiments for target chip which has highly symmetric structure. The entire system was designed in Virtuoso® Schematic Editor, using CSMC 0.5um DPTM PDK. The layout of the target chip and the Trojan was designed under Virtuoso® Layout Suite XL. Both the parasitic resistance and the capacitance of target chip were extracted by Calibre® using its PEX function. All the simulation curves were obtained by Spectre® with transient simulation mode.

The detection circuit is irrelevant to the function or statement, running or not, of the target chip, and is only related to its layout. So the function of the chip is non-significant. Fig .5 shows the layout of the target chip and the distribution of detection network. The target chip included two parts: the background circuit and the sensor chains. Background circuit was made of 6×6 array of inverter oscillators, with symmetric layout. As shown in Fig.5, each sensor chain consisted of 6 inverters with some interconnection wires, and were inserted using unused space. Twelve (0-5 and A-F) sensor chains were evenly distributed on the whole chip. Group I (0-5) are placed horizontally. Group II (A-F) are placed vertically. The chip was divided into 36 regions. The input pin of the whole sensor chain network, was placed in the top left of the chip, so the step activation signal can be put into the detection network. The entire target chip contains 792 transistors.

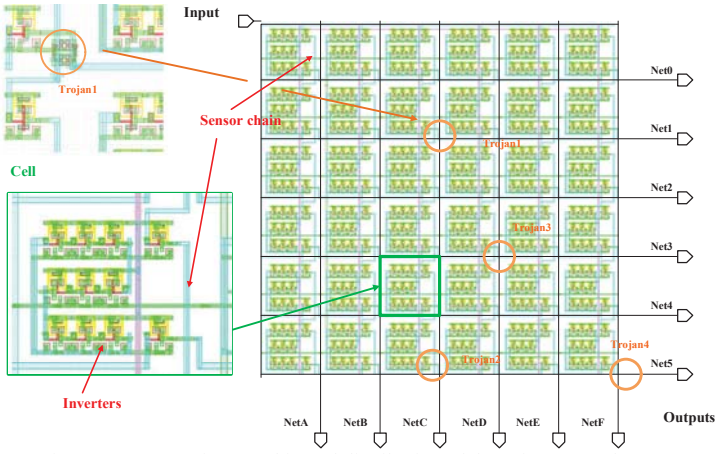


Figure 5. Layout of target chip and distribution of detection network

Because the Trojan will not be triggered for the most time, and its area is usually very small, the Trojan we inserted had only 4 minimum size transistors, and connected as dummy gates. To demonstrate the effectiveness of this method, we inserted the Trojan in four different positions in the target chip, respectively, as shown in Fig.5, in which the Trojan was abstract as an orange circle.

The pre-layout and post-layout simulation results of the Trojan-free chip are shown in Fig.6(a), and Fig.6(b), respectively. Zooming out the output curves of Fig.6(b) into Fig. 7(a1) and Fig. 7(a2), we could get the genuine ID of the target chip, which was {A,B,C,D,F,E} {0,1,5,3,2,4}.

In experiment 1, Trojan 1 was inserted, as shown in Fig.5. And the post-layout simulation output curves are shown in Fig.7(b1) and Fig7(b2).

Similarly, in the experiment 2-4, Trojan2-Trojan4 are inserted respectively, as shown in Fig.5. Each corresponding post-layout simulation results are shown in Fig.7(c1)/7(c2) – Fig. 7(e1)/7(e2).

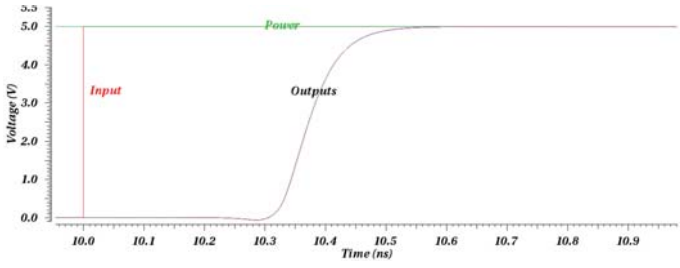
All the chip IDs obtained by RTD in experiment1 – experiment 4 are shown in Fig.8 and concluded in Table I. From Table I we can draw the following conclusions:

1) The ID of Trojan-inserted chip is different from the genuine ID, which means RTD can detect Trojan.

2) The changing ID numbers locate the Trojan.

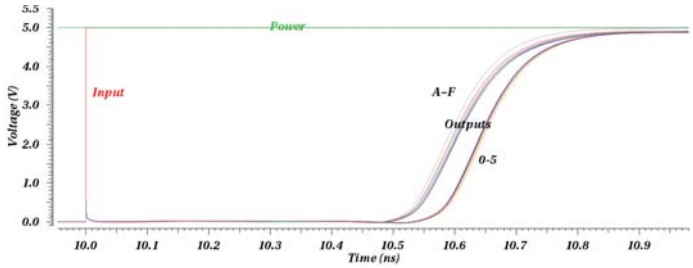
V. CONCLUSION

In this paper, a novel method for Trojan detection and location based on RTD is introduced. RTD is verified to be effective for Trojan detection, by four experiments. RTD needs no golden chip, besides that process variations and measurement noise will not influence the ID of the target chip, as well. For any chip with Trojan inserted，its chip ID will be changed. Moreover, this ID change can precisely indicate the location of the Trojan. Experiment results show that RTD is effective and precise.



(a)

Authorized licensed use limited to: Hong Kong University of Science and Technology. Downloaded on May 23,2023 at 02:25:44 UTC from IEEE Xplore. Restrictions apply.



(b)

Figure 6. (a)Pre-layout simulation results of Trojan-free chip (b) Post-layout simulation results of Trojan-free chip

TABLE I. CHIP IDS OBTAINED BY RTD

No.	Trojan Inserted Position	ID of Target Chip	Changed number
0	Trojan-free	{A,B,C,D,F,E}{0,1,5,3,2,4}	
1	(C,1)	{A,B,D,F,C,E}{0,5,3,2,1,4}	(C,1)
2	(C,5)	{A,B,D,F,C,E}{0,1,3,2,5,4}	(C,5)
3	(D,3)	{A,B,C,F,E,D}{0,1,5,2,4,3}	(D,3)
4	(F,5)	{A,B,C,D,E,F}{0,1,3,2,5,4}	(F,5)

ACKNOWLEDGMENT

This work was supported by the National Science and Technology Major Project of China under Grant 2017ZX01030301.

REFERENCES

[1] Wolff F, Papachristou C, Bhunia S, et al. Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme. Design, Automation and Test in Europe. IEEE:1362-1365, 2008.

[2] Zhang X, Tehranipoor M. RON: An on-chip ring oscillator network for hardware Trojan detection:1638-1643. 2011.

[3] Xiao K, Zhang X, Tehranipoor M. A Clock Sweeping Technique for Detecting Hardware Trojans Impacting Circuits Delay. IEEE Design & Test, 30(2):26-34, 2013.

[4] Xiao K, Tehranipoor M. BISA: Built-in self-authentication for preventing hardware Trojan insertion. IEEE International Symposium on Hardware-Oriented Security and Trust. IEEE:45-50, 2013.

[5] Rad R, Plusquellic J, Tehranipoor M. Sensitivity analysis to hardware Trojans using power supply transient signals. IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE:3-7, 2008.

[6] Kelly S, Zhang X, Tehranipoor M, et al. Detecting Hardware Trojans using On-chip Sensors in an ASIC Design. Journal of Electronic Testing, 31(1):11-26, 2015.

[7] Lecomte M, Fournier J J A, Maurine P. On-chip fingerprinting of IC topology for integrity verification. Design, Automation & Test in Europe Conference & Exhibition. IEEE:133-138, 2016.

[8] Agrawal D, Baktir S, Karakoyunlu D, et al. Trojan Detection using IC Fingerprinting. IEEE Symposium on Security & Privacy. IEEE:296-310, 2007.

[9] Jin Y, Makris Y. Hardware Trojan detection using path delay fingerprint. IEEE International Workshop on Hardware-Oriented Security and Trust. IEEE:51-57, 2008.

[10] Cao Y, Chang C H, Chen S. Cluster-based distributed active current timer for hardware Trojan detection. IEEE International Symposium on Circuits and Systems. IEEE:1010-1013, 2013.

[11] Rabaey J M, Chandrakasan A, Nikolic B. Digital Integrated Circuits, A Design Perspective, 2nd Prentice Hall. Englewood Cliffs, NJ, 2002.

Authorized licensed use limited to: Hong Kong University of Science and Technology. Downloaded on May 23,2023 at 02:25:44 UTC from IEEE Xplore. Restrictions apply.

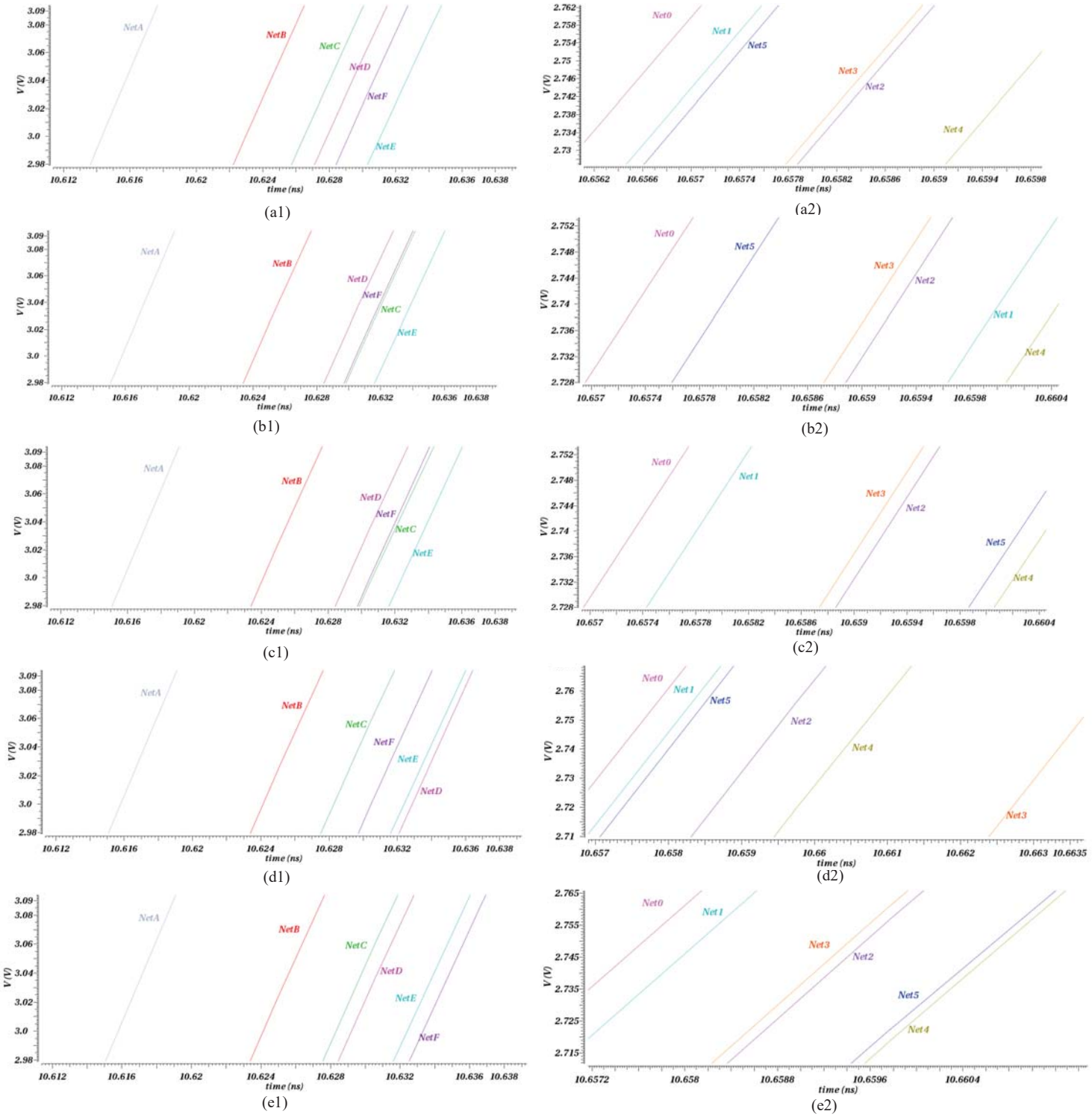


Figure 7. Zoomed out output curves in transient post-layout simulations.

(*1):NetA~NetF; (*2): Net0 ~ Net5; (a*) Trojan-Free; (b*) ~ (e*): Chip with Trojan1~Trojan4.

Authorized licensed use limited to: Hong Kong University of Science and Technology. Downloaded on May 23,2023 at 02:25:44 UTC from IEEE Xplore. Restrictions apply.