A Dummy Scan Flip-Flop Insertion Algorithm based on Driving Vertex

H L Liu1, a, L Li1, Z X Zhang2 and W T Zhou1
1 Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China
No.2006, Xiyuan Avenue, High-Tech West Zone, Chengdu, Sichuan, China
2 Taiwan Semiconductor Manufacturing Company (Nanjing)
No.16, Zifeng Road, Pukou Economic Development Zone, Nanjing, Jiangsu, China

a hailiangliu@std.uestc.edu.cn

Abstract. Commonly termed as Hardware Trojans, is an emerging issue for global hardware security. The research on Hardware Trojan detection is urgent and significant. Dummy Scan Flip-Flop (DSFF) structure could be used to improve the probability of hardware Trojan activation, which is significant to hardware Trojan detection, especially during the design phase. In this express, an algorithm for inserting the DSFF structure based on driving vertex is proposed. According to the experimental results, under the same transition probability threshold ($P_{th}$), compared to the state-of-art, the proposed algorithm can reduce both the inserting complexity and the induced area overhead of the DSFF insertion. The maximum area optimization rate can reach 44.8%. The simulation results on S386 and S38584 benchmark circuits indicate that the proposed algorithm can significantly reduce Trojan authentication time by increasing activation probability of hardware Trojan circuits.

1. Introduction
With the global expansion of the semiconductor industry, it has become a major challenge to ensure the trustworthiness of a given Integrated Circuit (IC). Commonly termed as Hardware Trojans, is an emerging issue for global hardware security in special application, such as military, economics, et al [1]. Hardware Trojans are kinds of extra and malicious circuits integrated in ICs spitefully, which could leakage information or change the original function, etc, and be a crucial threat for global information security [2].

As shown in figure 1, the basic structure of hardware Trojan is composed of two parts: the trigger and payload [3]. Generally hardware Trojan selects input signals from internal nets of main circuit to trigger the Trojan and modifies circuit function through Trojan payload. The significant characteristic of hardware Trojan is the low transition probabilities so that they can be dormant and have low influence on side channel signals such as power or delay. However, so long as the Trojan is trigged (fully or partially), the corresponding information can be used for Trojan detection using side channel analysis[4,5] or some other methods during the chip design phase.

The authentication time is the time consumed by confirming which a chip is attacked by hardware Trojan or not. In order to have an efficient detection and reduce Trojan authentication time, it's critical to:
Figure 1. The basic structure of Hardware Trojan

(i) Increase the probability of generating a transition in hardware Trojan;
(ii) Seek for effective detection methods to reduce the detection time.

To increase the activation probability of hardware Trojan circuit (i), hardware Trojan transition probability is modelled with geometric distribution [6] and a Dummy Scan Flip-Flop (DSFF) structure is proposed [8]. Inserting DSFF structure, it’s not only propitious to design test vectors to activate hardware Trojan in design phase but also conducive to generate test vectors to activate Trojan to increase the related side channel information during chip test phase [9, 10]. In a word, it is significant to increase the hardware Trojan activation probability.

This paper proposed a DSFF insertion algorithm based on driving vertex, which is shown in section 3. The proposed algorithm greatly reduces the insertion complexity and has lower effect on the circuit area. The rest of the paper is organized as follows: Section 2 presents the background of DSFF. The proposed algorithm, the new insertion procedure and the simulation results are described in Section 3. Section 4 concludes this paper.

2. Background of Dummy Scan Flip-Flop
This section describes the transition probability of the net modelled with geometric distribution [6] and the background of DSFF structure.

2.1. The transition probability and activation probability
In one clock cycle, assuming a net, the probability of which appears a logic 0 is $P_0$ and logic 1 is $P_1$. The transition probability of the net is defined as $P_t$ and modelled with geometric distribution [6], which is:

$$P_t = P_0 \times P_1$$

(1)

As a net is either logic 0 or logic 1, we have the following equation:

$$P_0 = 1 - P_1$$

(2)

According to the mathematical formula, it’s easy to know that only when $P_0 = P_1 = 0.5$, we can achieve the maximum probability of a net’s transition. When the probability of a net of logic 0 or logic 1 is close to 1, that is, $P_0 << P_1$ or $P_1 << P_0$, the transition probability of the net will be reduced dramatically.

A hardware Trojan may have the following conditions: 1) with low transition probability of nets; 2) rare combinations. Assuming the trigger circuit has q input ports, the probability of generating a specific trigger vector is:

$$P_{\text{trigger-vector}} = \prod_{i=1}^{q} P_i$$

(3)
where

\[
P_1 = \begin{cases} 
  P_{10} & \text{for trigger input Net}_i \text{ to be logic 0} \\
  P_{11} & \text{for trigger input Net}_i \text{ to be logic 1}
\end{cases}
\]  

(4)

From equation (3), we know that a trigger circuit could have several input ports and if \( P_1 \) is low, then the activation probability of the trigger circuit \( P_{\text{trigger-vector}} \) will be low. Therefore, to improve the activation of Trojan circuits, for each net of Trojan circuits, we should increase the transition probability of net(\( P_1 \)). During IC design phase, in order to improve the transition probability of nets, we need to insert DSFF structure at nets with transition probability lower than threshold \( P_{th} \).

### 2.2. The background of Dummy Scan Flip-Flop structure

The DSFF structure was proposed in paper [7] at first. Figure 2 shows two kinds of DSFF structures. DSFF is mainly include a scan chain which is made of one MUX and one Flip-flop, a gate (AND gate, OR gate) circuit with two input ports. SI is a test signal for MUX and TE is an enable signal.

![Figure 2. Two kinds of DSFF structures [7]](image)

If the probability of original circuit net logic value 1 is much higher than the logic value 0, selects the left DSFF structure, whereas selects the right DSFF structure. When the circuit works at normal mode, TE is logic 0, the value of nets don't change. When the circuit works at test mode, TE is logic 1, SI is a test input signal, the probability of logic 0 or logic 1 is 0.5. Then the probability of logic 0 or logic 1 in Q port of flip-flop is also 0.5. If \( P_0 << P_1 \) in the original circuit net, by inserting DSFF AND gate structure, we can improve the probability of logic 0; if \( P_0 >> P_1 \), we can also improve the probability of logic 1 by inserting DSFF OR gate structure. Therefore, DSFF structure could make a net's \( P_0 \) and \( P_1 \) become closer, which could improve the transition probability of a net.

### 3. The proposed algorithm

The inserted objects in the algorithm in the paper[8] are nets(stored in array M) with transition probability higher than \( P_{th} \). Then nets in M are sorted by transition probability in an increasing order and net with lowest probability is selected as target net which is to be inserted with DSFF structure. Next the number of low transition nets is judged. If the number is decreased, the inserted DSFF is kept, otherwise the DSFF would be ignored. As the quantity of M is \( N_{M} \), the insertion complexity is \( O(N_{M}) \).[8]

This express proposes a new DSFF insertion algorithm based on driving vertex. The driving vertex is defined as net located at the top of drive with transition probability lower than \( P_{th} \). Figure 3 shows the diagrammatic sketch of driving vertex.

From net M1 of the circuit topology, the transition probability of nets is lower than \( P_{th} \). So M1 is a driving vertex. M2 and M3 are drivers of M1.
Figure 3. The diagrammatic sketch of driving vertex

Shown as in figure 4, First, nets with transition probability lower than $P_{th}$ are stored in array L and all driving vertexes in L are stored in array T. Second, all drivers of driving vertexes are selected from nets with transition probability higher than $P_{th}$ and stored in array B. Third, all nets in array B are sorted by transition probability in an increasing order and the net with lowest probability is selected as target net and inserted with DSFF structure. Fourth, next target net will be selected and inserted with DSFF structure until the transition probability of all nets in the design are higher than $P_{th}$. The quantity of array B is $N_B$, so the insertion complexity of proposed algorithm is $O(N_B)$. Compared to paper[8], as $N_B<<N_M$, $O(N_B)<O(N_M)$. The proposed algorithm reduces the insertion complexity. Meanwhile, the proposed algorithm has a higher insertion efficiency and decreases the inserted quantity of DSFF, reduces the induced area overhead of DSFF insertion.

Figure 4. The new process of inserting DSFF structure
We choose S386 of ISCAS’89 benchmark circuit to verify the proposed algorithm. Table I lists the effect on circuit area of two insertion algorithms under different $P_{th}$. The proposed algorithm has a higher insertion efficiency and decreases the inserted quantity of DSFF, reduces the induced area overhead of the DSFF insertion.

As shown in table 1, we define a parameter $\eta = (\frac{(B-A)}{B} \times 100\%)$, which is to show the optimization on inserted DSFF circuit area that proposed algorithm makes relative to algorithm[8]. The maximum area optimization rate can reach 44.8%.

| $P_{th}$ | area percentage increase in proposed algorithm (A) | area percentage increase in [8] (B) | Area optimization rate $\eta = (\frac{(B-A)}{B} \times 100\%)$ |
|-------|-----------------------------------------------|---------------------------------|--------------------------------------------------|
| $10^{-5}$ | 7% | 9.3% | 24.8% |
| $10^{-4}$ | 7% | 12.7% | 44.8% |
| $10^{-3}$ | 14% | 19.7% | 28.9% |

To show the influence of inserted DSFF structure, the n32 and n42 nets with the lowest transition probability of the S386 benchmark circuit are selected for analysis. As shown in table 2, if n32 and n42 are attacked as input ports of a hardware Trojan, the transition probability of the net before inserting DSFF structure is 0.99999e-5. After inserting DSFF structure, the transition probability increases to 0.174, which is 4 orders of magnitude better than before.

| net | No DSFF | Inserted with DSFF |
|-----|---------|-------------------|
|     | $P_0$ | $P_1$ | $P_{n32}$ | $P_{n42}$ | $P_0$ | $P_1$ | $P_{n32}$ | $P_{n42}$ |
| n32 | 0.99999 | e-05 | 0.99999e-05 | 0.824 | 0.176 | 0.174 |
| n42 | 0.99999 | e-05 | 0.99999e-05 | 0.991 | 0.009 |

We select S38584 circuit of ISCAS’89 benchmark circuits as primary circuit. Under the condition of $10^5$ groups random test vectors, figure 5 and figure 6 show the transition in Trojan 1 circuit before and after inserting DSFF with the threshold value of $P_{th} = 10^{-5}$. n3937 and n3717 are internal nets of S38584 benchmark circuit with the transition probability less than $10^{-5}$, which are proper to be selected as access points of hardware Trojan. m1 is internal net of Trojan circuit and g29212 is the output of Trojan. Before the insertion of DSFF structure, the whole circuit keeps dormant until n3717 generates a transition at about $8 \times 10^9$ ps. After inserting DSFF, we can see in figure 6, g29212 is triggered several times and n3937, n3717, m1 generate a number of transitions within $2 \times 10^9$ ps. The transition probability of Trojan circuit nets is increased after the insertion of DSFF structure. So the activation probability of Trojan circuit is also increased according equation (1) and (3).

![Figure 5](image-url)
4. Conclusion
Hardware Trojan threat is becoming serious global security issues and research on hardware Trojan
detection is urgent and significant. In this express, we proposed a DSFF insertion algorithm based on
driving vertex. Compared to paper[8], the proposed algorithm can reduce both the DSFF structure
inserting complexity and the induced area overhead of the DSFF insertion. The maximum area
optimization rate can reach 44.8%. The simulation results on S386 and S38584 benchmark circuits
indicate that the proposed algorithm can significantly increase activation probability of hardware
Trojan circuits.

5. Reference
[1] Tony F. W, Karthik G, Yunqing Alexander H, H. -S. Philip W, Simon W and Subhasish M
2014 J. IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems 35 521-534
[2] Mingfu X, Wei L, Aiqun H and Youdong W 2014 J. IEICE Trans. Info E97-D 606
[3] Francis W, Chris P, Swarup B and Rajat S.C 2008 C. Int. Conf. on Design, Automation and Test
in Europe(Munich) (IEEE Conference Publications) p 1362-1365
[4] Seetharam N, Dongdong D, Rajat Subhra C, Somnath P, Francis G. W, Christos A. P, Kaushik
R and Swarup B 2012 J. IEEE Trans. on Computers 62 2183-2195
[5] Chenxu W, Jinghu L, Mingyan Y and Jinxiang W 2013 J. IEICE Electronics Express 10
20130602
[6] Dennis D. W, William M and Richard L. S 2008 B. Thomson Higher Education(Belmont,CA
94002-3098,USA)7th Chapter 3 140-149
[7] Hassan S, Mohammad T and Jim P 2009 Proc. Int. Workshop on Hardware-Oriented Security
and Trust (San Francisco) vol 9 (IEEE Press) p 66-73
[8] Hassan S, Mohammad T and Jim P 2012 J. IEEE Trans. on Very Large Scale Integration
Systems vol 20 (IEEE Press) p 112-125
[9] M. R, G. H, B V Bhargav R and Siva Y 2015 Proc. Int. Sym. on VLSI Design and Test (Hsinchu)
vol 19 (IEEE Press) p 1-6
[10] M. R, G. H and Siva Y 2015 Proc. Int. Conf. on Smart Technologies and Management for
Computing, Communication, Controls, Energy and Materials(Chennai) vol 1 (IEEE Conference
Publications) p 439-442

Acknowledgments
We are grateful for the relative research work done by related researchers and this work was supported
in part by the National Nature Science Foundation of China (Grant No.: U1630133).