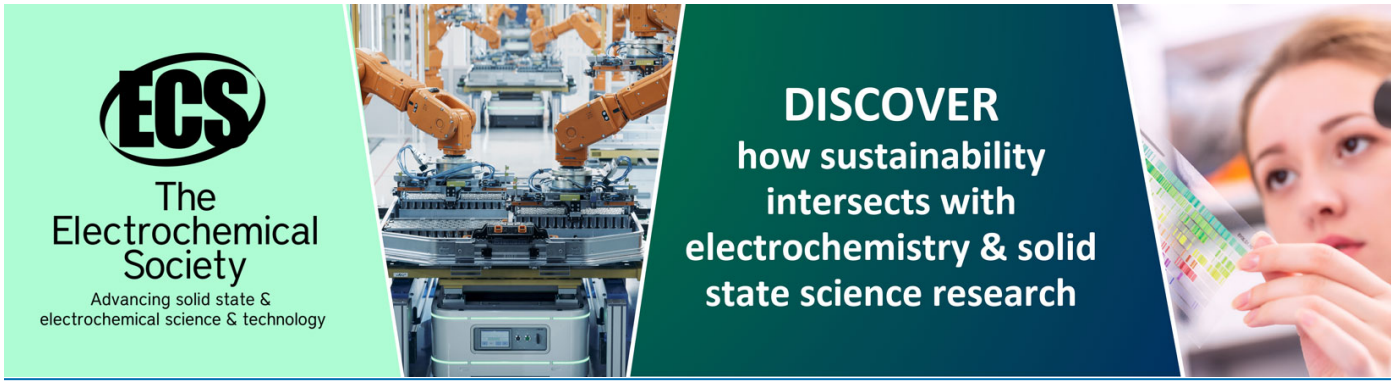
The optimized layout strategy of ring oscillator network for Trojan detection



IOP Conf. Series: Materials Science and Engineering **853** (2020) 012039 doi:10.1088/1757-899X/853/1/012039

The optimized layout strategy of ring oscillator network for Trojan detection

Lian Yang, Wenxiu Yang, Huan Li

University of Electronic Science and Technology of China; University of Electronic Science and Technology of China; University of Electronic Science and Technology of China

yanglian@uestc.edu.cn; 201821010626@std.uestc.edu.cn; photon_lee@uestc.edu.cn

Abstract. The method of Trojan detection based on the RON (Ring Oscillator Network) has been widely proposed and has a good effect. However, the method needs to integrate a RON on the chip to sense the voltage drop generated by the Trojan. Currently, the number of ROs (Ring Oscillator) required for a RON has not been discussed, which has a large impact on the additional hardware overhead. Therefore, based on the RON for Trojan detection, we propose an optimized layout strategy that can effectively control the number of ROs integrated into the circuit. By measuring the sensing range that can be perceived by a single RO, the sensing radius of the RO is obtained; then, ROs are placed in the circuit in a way of regular hexagonal lattice to clarify the number of ROs required in the network. Determining the appropriate number of ROs not only reduces the hardware overhead required for on-chip integration, but also ensures the reliability of Trojan detection, ensuring seamless coverage of the circuit with as few ROs as possible.

1. Introduction

Due to the separation of IC (Integrated Circuit) design and manufacturing, IC products are facing new security threats [1]. An attacker can insert a hardware Trojan at the design or manufacturing stage of an IC [2] to achieve the purpose of leaking circuit information, denial of service and so on [3]. There are endless methods of Trojan detection, most of which use the side channel information to distinguish the circuits with or without Trojans [4]. Since the ROs are distributed inside the circuit, they are able to generate signatures more accurately than other side-channel methods.

After the method of Trojan detection based on the RON was proposed, some research based on the method also appeared. But there has been no discussion of the number of ROs required in a RON. Such a discussion is obviously necessary, because how to reduce the resource overhead is an important issue. In this paper, we propose an optimized layout strategy for a RON. By optimizing the layout method and determining the suitable number of ROs, the entire circuit or system can be seamlessly covered with as few ROs as possible.

2. Related work

In the past research work, the researchers put forward lots of methods about RON to detect hardware Trojans.

2.1. The methods of the Trojan detection based on RON

Zhang *et al*. first proposed the technique of detecting hardware Trojans by integrating RON on the on-chip in [5]. They pointed out that RO effectively reduces the influence of noise on the side channel information. The method can implement Trojan detection in the test stage by analyzing the data of ROs. In addition, the RON can also be applied to the real-time defense system of Trojan detection, which alerts when the Trojan is activated, thus providing the last strong barrier for the hardware circuit [6-7].

2.2. The layout of RON

In the past research, there are two common layouts: "Mesh" layout [8-9] and "X" layout [10]. However, neither of the two layouts considers the sensing range of the RO, and the seamless coverage of the sensing range cannot be realized, so that the correct rate of the Trojan detection cannot be reliably guaranteed. Wu *et al*. pointed out that the circles of the same radius completely can cover a plane and the optimal layout with the farthest distance between the centers is a hexagonal grid [11]. This ensures that as few circles as possible are used to seamlessly cover a plane, providing a strong basis for our approach.

3. Our method

We will explain our approach in three ways: determining the coverage radius of the RO, the layout strategy, and determining the number of ROs.

3.1. Determining the coverage radius of the RO

Assuming that the frequency of an RO is F. Due to the actual measurement and the influence of noise, for a circuit without Trojans (H_0), F should satisfy the Gaussian distribution with mean u_0 and variance σ_0. Similarly, for circuits infected with Trojans (H_1), the frequency F should satisfy the Gaussian distribution with mean u_1 and variance σ_1.

The Trojan analog circuit is placed at a position away from the RO by i(i=1,2,…) slice. At this time, the frequency values of the RO are recorded as a Gaussian distribution with mean u_1^i and variance u_1^i($=\sigma_0$). The coverage radius of the RO is Equation 1.

$$r = \max\left(\left\{i \,|\, \left|\mu_0 - \mu_1^i\right| \geq \sigma_0\right\}\right) \tag{1}$$

3.2. The layout strategy

Due to the size of circuit is limited, we will discuss the boundary condition of the circuit. The size of the circuit C is $x \times y$, the measured coverage radius of the RO in the previous section is r.

3.2.1. ROs are laid out according to regular hexagon grid division.

The circuit is subjected to regular hexagonal meshing with the lower left corner of the circuit as the origin. The regular hexagon here is an inscribed regular hexagon of a circle of radius r. Here, a regular hexagon is placed laterally so that the lower left corner is aligned with the origin, and the bottom edge is aligned with the x-axis. Based on the regular hexagon, the adjacent regular hexagon can be found, and then the adjacent regular hexagon is used as a reference. Find the regular hexagons adjacent to them, and so on, until the circuit is completely covered. If the ROs are placed in the center of these grids, seamless coverage of the circuit can be achieved.

The problem is that after the regular hexagonal mesh is divided, some of the grid's center position will be beyond the circuit range. For the position of the edge ROs, adjustments need to be made to make it inside the circuit.

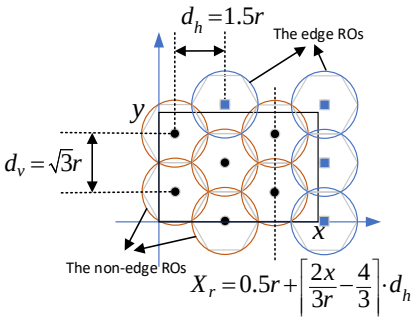


Figure 1. The schematic of Non-edge and edge ROs.

To facilitate description, some symbols are defined and are labeled in Figure 1. Here, the x-coordinate of non-edge ROs in the rightmost column is denoted as $Xr=0.5r+\left\lfloor\frac{2x}{3r}-\frac{4}{3}\right\rfloor\cdot d_h$. The distance between the ROs is recorded as $d_v=\sqrt{3}r$, and the distance between the two columns is recorded as $d_h=1.5r$. Since the number of non-edge ROs of odd and even columns may be different, the number of odd and even non-edge ROs is $N_o=\left\lfloor\frac{y}{d_v}-\frac{1}{2}\right\rfloor+1$ and $N_e=\left\lfloor\frac{y}{d_v}\right\rfloor+1$, and the number of columns of odd and even columns is $M_o=\left\lceil\frac{x}{2d_h}-\frac{7}{6}\right\rceil+1$ and $M_e=\left\lceil\frac{x}{2d_h}-\frac{5}{3}\right\rceil+1$.

Here, the position of the non-edge ROs are inside the circuit, which are fixed in the following discussion, and the position of the odd column non-edge ROs are given as Equation 2.

$$\left(0.5r+m_o\cdot 2d_h,0.5d_v+n_o\cdot d_v\right) \tag{2}$$

Where the range of m_o is from 0 to M_o-1 and the range of n_o is from 0 to N_o-1.
Similarly, the position of the even column non-edge ROs are Equation 3.

$$\left(2r+m_e\cdot 2d_h,n_e\cdot d_v\right) \tag{3}$$

Where the range of m_e is from 0 to M_e-1 and the range of n_e is from 0 to N_e-1.

3.2.2. Adjusting the position of the edge ROs.
The edge ROs have exceeded the range in which the circuit can be laid out, so the position of the edge ROs need to be re-adjusted.
Situation 1: The edge ROs exist outside the upper boundary of the circuit.
Given this case, the position coordinates of the upper edge RO after adjustment are as shown in Equation 4.

$$\begin{cases}\left(0.5r+m_o\cdot 2d_h,y\right), & 0<x-X_r\le 0.5r,0<y\ \%\ d_v<\ 0.5d_v\\ \left(2r+m_e\cdot 2d_h,y\right), & 0<x-X_r\le 0.5r,0.5d_v<y\ \%\ d_v<d_v\end{cases} \tag{4}$$

Situation 2: The edge ROs exist outside the right edge of the circuit.
Give adjusted position coordinates of the right edge ROs as Equation 5.

$$\begin{cases}\left(X_r+0.5r,0.5d_v+n_o\cdot d_v\right), & 0.5r<x-X_r\le r,y\ \%\ d_v=0 \text{ or } 0.5d_v\\ \left(X_r+r,0.5d_v+n_o\cdot d_v\right), & r<x-X_r\le 1.5r,y\ \%\ d_v=0 \text{ or } 0.5d_v\end{cases} \tag{5}$$

3.3. Determining the number of ROs
We can give the number of ROs required to completely cover the circuit C of the size $x\times y$ using the ROs of radius r. The situation can be reduced to Equation 6 when calculating the number of ROs.

$$Num_{RO}=\begin{cases} M\cdot N, & 0<y\ \%\ d_v\le 0.5d_v \\ M\cdot\left(\left\lfloor\frac{N}{2}\right\rfloor+1\right)+(M+1)\cdot\left(\left\lceil\frac{N}{2}\right\rceil-1\right), & others \end{cases} \tag{6}$$

Where M is equal to $\left\lceil\frac{y}{d_v}\right\rceil$ and N is equal to $\left(\left\lceil\frac{x-r}{d_h}\right\rceil+1\right)$.

4. Experimental results

4.1. Perceptual radius and number of ROs

For comparison, Reference [8] uses a 4×2 ROs array (the low-density layout), a similar 4×3 ROs array (the high-density layout) is used in [9], and the literature [10] uses 32 ROs which were distributed on the diagonal of the circuit (the X-shaped layout). Table 1 summarizes the size of the underlying circuit, the measured coverage radius of the RO, and the number of ROs required by our method.

Table1. The coverage radius and quantity statistics of ROs.

The name of the base circuit	The size of circuit (Slice)	Perceptual radius of RO(Slice)	The number of ROs
AES	30×30	7	12
BasicRSA	18×18	4	13
Memctrl	26×26	7	9
Wb_conmax	40×48	11	10
MC8051	32×32	9	7

The number of ROs required for our method is less than the low-density layout in the MC8051 basic circuit, and more ROs are required in the other test circuits than the low-density type. In addition, compared with the high-density layout, the method in this paper uses more ROs in two of the test circuits, four test circuits use less RO, and the remaining four test circuits have the same number of ROs as the high-density type.

4.2. The accuracy of Trojan detection

The accuracy of Trojan detection is shown in Figure 2.

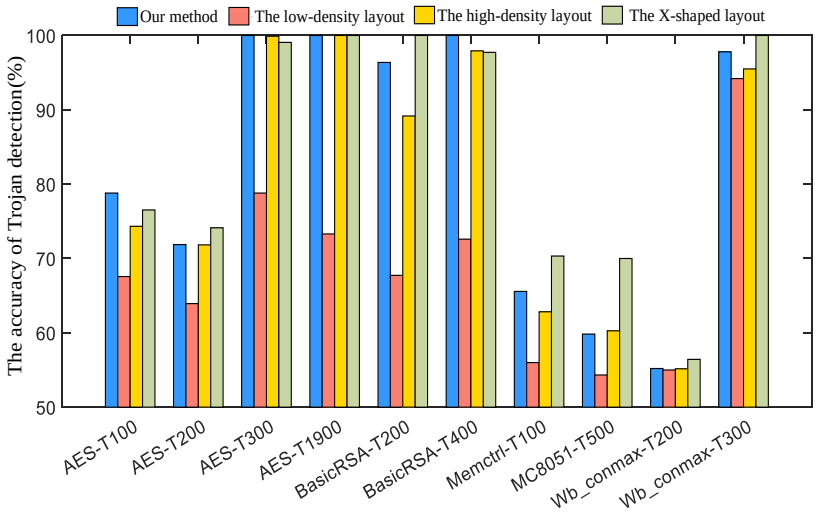


Figure 2. The accuracy result of Trojan detection.

As shown in Figure 2. It can be found that the results of the low-density layout are lower than the other three methods in all the test circuits. In addition, the high-density layout is also inferior to the method proposed in this paper. Beyond that, the methods proposed in this circuit with more than 1% of Trojans have the accuracy of over 95%. In addition to this, because our method can realize the full range sensing of the circuit, the detection rate of the Trojan is relatively stable, while other methods have coverage gaps, and the accuracy of the Trojan changes with the position of the Trojan. In actual situations, the location of the Trojan is unknown, which reflects the advantages of our approach.

5. Conclusion

In this paper, an optimized method for the number of ROs in the network is proposed. The method first gives the actual measurement method of the sensing range. On this basis, we propose a RON layout method based on regular hexagonal meshing. This method can achieve seamless coverage of the circuit. The method proposed in this paper was verified by experiments on 10 test circuits, and the number of ROs and Trojan detection effects in the layout used in other literatures were compared. Experiments show that the proposed method can guarantee the correct rate of Trojan detection with fewer ROs.

References

[1] M. Tehranipoor, C. Wang. Introduction to hardware security and trust[M]. New York: Springer, 2011, 339-364.
[2] B. Shakya, T. He, H. Salmani, *et al*. Benchmarking of hardware Trojans and maliciously affected circuits[J]. Journal of Hardware and Systems Security, 2017, 1(1): 85-102.
[3] M. Tehranipoor, C. Wang. Introduction to hardware security and trust[M]. New York: Springer, 2011, 325-338.
[4] D. Agrawal, S. Baktir, D. Karakoyunlu, *et al*. Trojan detection using IC fingerprinting[C]. 2007 IEEE Symposium on Security and Privacy (SP'07), Oakland, 2007: 296-310.
[5] X. Zhang, M. Tehranipoor. RON: An on-chip ring oscillator network for hardware Trojan detection[C]. 2011 Design, Automation & Test in Europe, Grenoble, 2011: 1-6.
[6] C. Bao, D. Forte, A. Srivastava. On application of one-class SVM to reverse engineering-based hardware Trojan detection[C]. International Symposium on Quality Electronic Design, Santa Clara, 2014, 47-54.
[7] D. Forte, C. Bao, A. Srivastava. Temperature tracking: An innovative run-time approach for hardware Trojan detection[C]. International Conference on Computer-Aided Design, San Jose, 2013, 532-539.
[8] S. Kelly, X. Zhang, M. Tehranipoor, *et al*. Detecting hardware trojans using on-chip sensors in an asic design[J]. Journal of electronic testing, 2015, 31(1): 11-26.
[9] X. Zhang, M. Tehranipoor. RON: An on-chip ring oscillator network for hardware Trojan detection[C]. 2011 Design, Automation & Test in Europe, Grenoble, 2011: 1-6.
[10] C. Lamech, R. M. Rad, M. Tehranipoor, *et al*. An experimental analysis of power and delay signal-to-noise requirements for detecting Trojans and methods for achieving the required detection sensitivities[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 1170-1179.
[11] C. W. Wu, D. Verma. A sensor placement algorithm for redundant covering based on riesz energy minimization[C]. 2008 IEEE International Symposium on Circuits and Systems, Seattle, 2008: 2074-2077.