Research on physical unclonable functions circuit based on three dimensional integrated circuit

Ni Tianming¹, Chang Hao², Zhang Xiaoqiang¹, Xiao Hao³, and Huang Zhengfeng³a)

1 College of Electrical Engineering, Anhui Polytechnic University, Wuhu 241000, China
2 Department of Computer Science and Technology, Anhui University of Finance and Economics, Bengbu 233030, China
3 School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230009, China
a) huangzhengfeng@139.com

Abstract: As the mainstream technology of the next generation chip design, to ensure the information security of three dimensional integrated circuits (3DIC) is very necessary, however, the existing hardware security technology is still not suitable for 3DIC’s unique stack structure and interconnection technology. This paper proposes a novel Physical Unclonable Functions (PUF) circuit technology based on 3DIC. The new scheme exploits the process variation of both CMOS devices and TSVs (Through Silicon Vias) available on TSV-based 3DIC, for secure data generation resistant to physical attacks. In the six layers of the 3DIC, the TSV-based ring oscillator PUF Circuit and independent arbiter PUF circuit are designed. The TSV is introduced as additional sources of process variation, and the same 100 3DIC-PUF chips are simulated through HSPICE under the process variation pre-set. The simulation results show that the TSV-based PUF circuit has good unique and reliability, and can be directly applied to the field of 3DIC security authentication.

Keywords: 3DIC, TSV, PUF, process variation

Classification: Integrated circuits

References

[1] T. Ni, et al.: “Vernier ring based pre-bond through silicon vias test in 3D ICs,” IEICE Electron. Express 14 (2017) 20170590 (DOI: 10.1587/elex.14.20170590).
[2] T. Ni, et al.: “A region-based through-silicon via repair method for clustered faults,” IEICE Trans. Electron. E100-C (2017) 1108 (DOI: 10.1587/transele.E100.C.1108).
[3] MD. T. Rahman, et al.: “An aging-resistant RO-PUF for reliable key generation,” IEEE Trans. Emerg. Top. Comput. 4 (2016) 335 (DOI: 10.1109/TETC.2015.2474741).
1 Introduction

The advent of three-dimensional integrated circuit (3DIC) technology has opened up the potential of highly improved circuit designs. Through silicon vias (TSVs) enable the vertical integration of separate dies to form a single 3D chip. The TSV-based 3D stacking technology promises better performances, including smaller footprint, higher bandwidth, lower power and higher interconnect density [1, 2].

However, the research on 3DIC from the perspective of hardware security is still relatively few. As the mainstream chip design in the future, it is necessary to ensure the security of its application.

Against physical attacks on secret keys, the Physical Unclonable Function (PUF) is an effective technology based on an intrinsic physical characteristic of an IC for authentication, cryptographic secret key generation, and Intellectual Property (IP) protection [3, 4, 5, 6, 7]. PUF utilizes the impact of CMOS technology process variations on delay circuits or matched bi-stable storage cells to derive secret responses, thus PUF has more advantages over traditional chip encryption methods.
in terms of safety performance. In the past decade, many conventional PUFs including arbiter PUFs, RO (Ring Oscillator) PUFs, DFF PUFs, Latch PUFs, and SRAM PUFs have been reported [4, 5, 6, 7, 11, 12]. Wang [13] pioneerly carried out a ring oscillator based PUF in 5-layers 3DIC, and the difference between 3DIC-PUF and traditional PUF is analyzed. It pointed out that the safety performance of 3DIC-PUF is better than that of traditional PUF by introducing the deviation of TSV technology. Motivated by the emerging TSV-based 3D integration technology and PUF circuits, two novel RO-based and arbiter-based 3DIC-PUF circuits making use of both CMOS and TSV process variation in multiple die stack are proposed. To the best of our knowledge, there are few previous works on arbiter-based PUF circuits in 3DIC.

In this paper, we propose two kinds of novel 3DIC-PUFs, namely RO-based and arbiter-based, which are capable of producing reliable responses for authentication and secure key generation. A typical hybrid 3DIC is a stack of multiple ICs vertically connected by many TSVs, which performs sensing, computing, and transmitting. By re-using the TSVs available in the stack, inverters across multiple dies can be formed and grouped to make 3D RO-based or arbiter-based PUF circuits to generate stable responses with stronger uniqueness and reproducibility by exploiting the additional process variation and capacitive loading from the TSVs.

The rest of this paper is organized as follows. Section 2 discusses the background of TSV process variation. Section 3 proposes the RO-based and arbiter-based 3DIC-PUFs. Section 4 presents simulation results and analysis on the proposed 3DIC-PUFs. Finally, Section 5 concludes this paper.

**2 Analysis of TSV process variation**

TSV is deeply embedded in the substrate, thus its manufacturing process is much more complex than traditional metal interconnects. The manufacturing process of TSV includes deep etching, deposition of oxide layer, diffusion and growth of crystal layer, metal copper filling and final chemical mechanical planarization process. Therefore, due to the limitation of manufacturing technology, the final process variation of TSV is much more serious than that of traditional metal wire [8, 9]. The main material of the TSV technology is copper, its diameter is 5 µm, and the height is 50 µm. Due to the relatively simple process of the traditional interconnect, the delay variation caused by the process is weak, so the existing PUF mainly uses the delay difference caused by the process variation of the transistor. Therefore, when the addition process variation of TSV is introduced into the PUF circuit, it will greatly enhance the reliability of the PUF circuit.

Traditional PUF mainly realizes the unclonable characteristic of PUF through the difference of circuit delay caused by the process variations of transistors. When transistor is used as the source of process variation, its delay characteristic is indirectly reflected mainly by the change of threshold voltage and channel length caused by process variation. When the TSV is used as the source of process variation, the change of resistance capacitance caused by its process variation will dominate the delay characteristics. As illustrated in Fig. 1, the TSV needs a driving
cell to drive in the circuit, the actual TSV delay model can be assumed to be shown in Fig. 2, \( R_d \) and \( C_d \) are the equivalent resistance and capacitance of driving cell, respectively. On the other hand, \( R_{tsv} \) and \( C_{tsv} \) are the equivalent resistance and capacitance of TSV, respectively. Thus, the delay can be calculated as follows:

\[
T_{\text{Delay}} = \frac{R_d}{C_d} + \left( \frac{R_d + R_{tsv}}{C_{tsv}} \right) \quad (1)
\]

In order to study the delay fluctuation caused by the process variation of both the transistors and TSVs, 100 Monte Carlo simulations of TSV delay model (the process deviation is set to 10%) are carried out under the 45 nm CMOS process. The resulting delay result, as shown in Fig. 3, shows that the delay fluctuation caused by the process deviation is much more intense than the traditional inverter chain, and it has strong randomness.

The specific results are as follows: the mean time delay of the TSV is 169.1 ps, the standard deviation is 15 ps, the maximum value is 200.7 ps, and the minimum value is 131.5 ps; the mean time delay mean of the inverter is 7 ps, the standard deviation is 0.7 ps, the maximum value is 8.6 ps, and the minimum value 5.5 ps. The inherent delay and delay fluctuation are both greatly improved after introducing TSV. Therefore, introducing TSV as an additional source of process deviation will greatly enhance the safety performance of PUF.

3 Proposed 3DIC-PUF circuits

The design of the conventional RO-based PUF must keep the RO composed of a long loop. One reason is that only a long loop can bring enough delay so that a
relatively small oscillation frequency can be obtained to meet the precise counting requirements of the sampling count. In addition, a very long loop means more devices, which ensures that the distribution of the process variation of the whole circuit is large enough to bring enough delay difference for different ROs. For traditional arbiters, PUF also needs a long link to ensure that the final delay difference is large enough to meet sampling and comparison. It is known from the above section that the introduction of the TSV not only increases the inherent delay of the circuit, but also has strong randomness and great fluctuation when the process variation exists. Therefore, the introduction of TSV can solve the above problems, reduce the hardware cost and reduce the power consumption. Combining the process variation between transistors and TSVs, 3DIC-PUF circuits are realized. According to the characteristics of the 3DIC, the traditional RO-based PUF and the arbiter-based PUF are re-designed, so that they can be well applied to the stacking structure of the 3DICs.

Based on the existing RO-based PUF circuit structure, a circular TSV-based RO PUF is designed based on the delay characteristic of the TSV. The specific circuit structure is shown in Fig. 4. A 3DIC is made up of six layers of die stacking, and the interconnection between two adjacent dies is completed by TSVs. That is to say, TSV is used instead of traditional metal interconnect, and TSV is the signal transmission line between layer and layer in 3DICs. The shadow part in Fig. 4 is the six layers, and the black signal line between the chip and the chip is the TSV. Through the top layer, TSV is connected to each layer in turn and then connected upwards to the top layer. Finally, a complete RO is composed of ten TSVs, ten inverters and one NAND gate. In the design, the whole PUF circuit contains 256 identical ROs, which have similar structure and layout wiring. The same node at the top layer in all ROs is connected to the multi-channel selection module. A pair of ROs is selected by selecting the control signal, and the counter is counted by the counter. Finally, the two values are compared and a bit response bit is output. The selection module, counter and comparator are all on the top layer. And the specific implementation of module, counter and comparator is not selected in detail.

![Fig. 4. TSV-based RO PUF.](image-url)
Next, the operation steps of the ring oscillator PUF circuit are explained in detail. Firstly, two ROs that will be compared are selected by configuring two multiplexers. At this time, the two selected ROs are connected to the counters respectively. Then, the autonomous oscillation of the RO is started by setting ‘1’ on the remaining input pin (oscillation enable) in the selected two ROs. Finally, after oscillation stabilization, the oscillating frequency is recorded through the counter, and then the result is transmitted to the comparator, and the final response bit is output after comparison. By using the same method to select different ring oscillators, a set of output response sequences can be obtained. For example, first choose 1 and 129 to compare, then select 2 and 130, and so on, until 128-bits response output sequence is obtained.

Fig. 5. TSV-based independent path arbiter PUF.

In order to ensure the reliability of the PUF circuit, the traditional arbiter-based PUF circuit needs more stages to make the delay difference of the two paths large enough. In the 3DIC, the combination of transistor and TSV makes it possible to use less stages to make the delay difference of the two path meet the reliability requirements. The independent path arbiter PUF based on TSV is designed in this paper. The specific circuit structure is shown in Fig. 5. Similarly, for the 6-layer 3DIC, the required PUF circuits are realized by inverters, TSVs, multiplexers and arbiters. The input signal is transmitted from the top layer to the next layer through the TSV, then it arrives at the bottom and then returns. After 10 stages, it reaches the MUX selector on the top layer, and the final result is output by the arbiter. The same path is copied by 256 copies, so that a large number of input and output response pairs can be obtained by controlling MUX input signal. The independent path arbiter PUF changed the multi-level MUX path selection operation in the traditional arbiter PUF, and it used the selection structure similar to the RO. Therefore, the same as the RO PUF, the independent path arbiter PUF has the advantage of easy to implement and evaluate the entropy easily on the ASIC and FPGA. In addition, similar to traditional arbiter PUF, it has the advantages of the fast speed, small area overhead and low power consumption.
The specific operation steps are similar to the RO-based 3DIC-PUF. Firstly, the multiplexer is configured to select two links that will be compared, which is connected to the two input of the arbitrator respectively. Then the link input is changed from 0 to 1, and the rising edge is propagated in the link to compare the propagation speed in the two links. Finally, the result of comparison is obtained from the arbiter. By repeating the above steps and selecting different links, we can get a set of output response sequences.

4 Simulation result and analysis

In this paper, under the PTM 45 nm CMOS process library, the proposed two kinds of 3DIC-PUF circuits based on TSVs are simulated and tested by HSPICE. Through Monte Carlo simulation, 100 different chips are generated, containing the same PUF circuits on each chip. In the experiment, the process variation is reflected by the fluctuation of the transistor channel length $L$ and the $RC$ of the TSV. They obey the corresponding Gauss distribution (the relative change is 10%, the standard deviation is 3). Each RO-based PUF and arbiter-based PUF generates 128-bits output response. The experimental standard voltage is 1.1 V, and the temperature is 25°C at room temperature. Next, we verify the uniqueness and reliability of the output response of 3DIC-PUF circuit.

4.1 Uniqueness

Uniqueness reflects the difference of output response produced by the same PUF circuit on different chips under the same excitation. Generally, the PUF uniqueness is evaluated by the average Inter-Die Hamming Distance for a group of $N$ chips [10], which is described by

$$Uniqueness = \frac{2}{N(N - 1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \frac{HD(R_i, R_j)}{l} \times 100\%$$

where $R_i$ and $R_j$ are the $l$-bit secret responses extracted from the different chip $i$ and $j$, respectively. The equation includes all possible pair-wise HDs among the $N$ chips.

In order to verify the uniqueness of the proposed PUF circuit, 128-bits output response is obtained by inputting the same signal to PUF circuit of each chip. The output response of the 100 chips is statistically processed, and the results are shown in Fig. 6. The X-axis represents the inter-die Hamming distance between two PUF output responses, the Y-axis indicates the frequency of the occurrence, and the black curve is the distribution curve generated by the fitting of the experimental results. The graphical results clearly reflect the Hamming distance distribution between the responses of the 128-bits output of the 100 circuits. According to Fig. 6(a) and formula (2), the uniqueness of the RO-based 3DIC-PUF is 49.94%, and the mean value of the Hamming distance between the 128-bits output responses is 63.92. Similarly, according to Fig. 6(b), we can figure out that the uniqueness of the independent path arbiter PUF is 49.88%, and the average value of the 128-bits output response is 63.85. In the ideal case, the uniqueness result is 50%, and the average inter block Hamming distance of the output response is 64. Therefore, it
can be concluded that the two PUF circuits designed in this paper have very good uniqueness.

4.2 Reliability

The reliability of a PUF quantifies the reproducibility of PUF response to the same challenge from a die/chip over varying operating or environment condition. The PUF reliability is estimated by the average intra-die Hamming Distance (Intra-HD) over \( S \) samples of response \( R_i \) from a chip \( i \) [10], which is defined as,

\[
\text{Reliability} = \frac{1}{S} \sum_{p=1}^{S} \frac{\text{HD}(R_i, \tilde{R}_{i,p})}{I} \times 100\%
\]

where \( R_i \) is the \( I \)-bit reference response extracted from the chip \( i \) at the normal operation condition, and \( \tilde{R}_{i,p} \) is the \( p \)-th sample of \( R_i \) in a different operation condition.

In order to verify the reliability of proposed PUF circuits, 18 different environmental changes were simulated. The voltage is 1.0 V, 1.1 V and 1.2 V, respectively, and the temperatures are 0, 25, 50, 75, 100, 125, respectively. The experimental standard voltage is 1.1 V, and the temperature is 25°C at room temperature. Under different voltage and temperature environment, the same excitation is input to the PUF circuit, and finally the output responses are compared with the output response under standard conditions. The experimental result is shown in Fig. 7. The X-axis is the number of errors in the 128-bits output response, and the Y-axis is the number of occurrence times. When the voltage and temperature change, an error below 5 bits will appear in the output response. The average Hamming distance of the 128-bits output response of the RO-based PUF is 2.78 and the reliability is 2.2%; and the average value of the Hamming distance in the 128-bits output response of the arbiter-based PUF is 1.94 and the reliability is 1.5%. The ideal reliability result

![Fig. 6. Inter-chip hamming distance probability distribution for 3DIC PUF circuits.](image)

![Fig. 7. On-chip hamming distance probability distribution for 3DIC PUF circuits.](image)
should be 0%, and the average inter block Hamming distance of the output response is 0. Therefore, it can be concluded that the reliability of the two PUF circuits designed in this paper is also very good.

### 4.3 Comparison and analysis

The uniqueness and reliability of the RO-based PUF circuit and the independent path arbiter-based PUF circuit are obtained through simulation experiments. In order to compare the performance of the PUF circuit with the traditional chip more directly, the traditional PUF refers to the most basic RO PUF and the arbiter PUF, and there is no use of any auxiliary design of the original circuit. In this paper, the same experiments have been carried out for the traditional RO PUF and arbiter PUF, and their corresponding uniqueness and reliability have been obtained. At the same time, it is compared with other methods as shown in Table I.

| Methods       | Type  | Realization | Uniqueness | Reliability |
|---------------|-------|-------------|------------|-------------|
| 2007 DAC [5]  | RO    | FPGA        | 46.15%     | 0.48%       |
| 2015 TCAD [11]| RO    | ASIC        | 50.42%     | 2.78%       |
| 2016 TVLSI [12]| Arbiter | ASIC      | 50.04%     | 3.2%       |
| Traditional PUF | RO    | HSPICE | 49.84% | 0.74% |
| Arbiter     | HSPICE | 50.03% | 1.22% |
| 3D-PUF      | RO    | HSPICE | 49.94% | 2.2% |
| Arbiter     | HSPICE | 49.88% | 1.5% |

It can be seen that the reliability and uniqueness of all PUF circuits are very high, which basically can meet the requirements of safety performance in practical use. However, as mentioned before, 3D-PUF has greater process variation, which will lead to more obvious delay fluctuations. In this way, the larger delay difference in the actual chip will be more insensitive to the environmental changes, and the PUF circuit is more stable. For example, the frequency range of the traditional RO is 171.5 ps~203.5 ps, that is, the optimal period of the two RO is only 32 ps, which is too high for the counting and comparison circuits. However, the period range of RO in 3D-PUF is 4.331 ns~5.181 ns, and the largest period difference is 850 ps. A larger period difference provides more redundancy guarantees for PUF’s security and it is also easier to get corresponding output response bits. According to the existing experience, there will be a big difference between the CAD simulation results and the actual chip, that is, the uniqueness and reliability of the actual chip will generally be much worse than expected, and the larger periodic fluctuation in the 3D-PUF can greatly reduce this difference.

### 5 Conclusion

In this paper, two kinds of novel TSV based PUF circuits are proposed for 3DIC. By using the larger inherent delay and process variation of the TSV, the RO-based
PUF circuit and the independent path arbiter-based PUF circuit are realized. Under the 45 nm CMOS technology, 100 PUF chips with 128-bits output response were simulated. The experimental results show that the uniqueness of the RO-based PUF and the independent path arbiter-based PUF are 49.93% and 49.88% respectively, and the reliability is 2.2% and 1.5% respectively. It is proved that the 3DIC-PUF based on TSV has good uniqueness and reliability, and it can be applied to the information security authentication field of 3DIC.

Acknowledgments

This paper is supported by National Nature Science Foundation of China under grant No. (61574052, 61504059, 61704001), Anhui Provincial Natural Science Foundation under grant No. (TSKJ2017B23, 1808085QF196), and the initial funding of Anhui Polytechnic University under grant No. (2018YQQ007, 2017YQQ001) and Key projects of Natural Science Research of universities in Anhui Province under grant No. KJ2016A001.