

Diffusion Programmable Device : The device to prevent reverse engineering

Mitsuru Shiozaki, Ryohei Hori and Takeshi Fujino *

February 2014

Abstract

The secret information, which is embedded in integrated circuit (IC) devices such as a smart card, has the risk of theft by reverse engineering (RE). The circuit design of IC can be stolen by the RE, and the counterfeit can be illegally fabricated. Therefore, the secure IC device requires the circuit architecture protected from the RE attacks. This paper proposes the diffusion programmable device (DPD) architecture as a countermeasure against the RE. A look-up table circuit based on the DPD can generate desired logic function without changing the layout except diffusion layer. And, the logic function can be programmed by assigning the N-type or P-type dopant to a part of active region. A test chip using the DPD-LUT was prototyped with a 180nm CMOS technology. And, operations of various logic functions such as AND, OR, XOR and XNOR were confirmed through experiments.

Keywords: Reverse engineering, Countermeasure, Diffusion programmable device (DPD)

1 Introduction

Recently, secret information is embedded in several integrated circuit (IC) devices such as a smart card. The secret information has the risk of theft by reverse engineering (RE) [1] [2]. In the RE attack, an attacker obtains the circuit design information by analyzing the layout regularity of each logic gate [3]. Furthermore, an attacker can illegally fabricate counterfeit IC by utilizing the stolen information. Therefore in order to protect the secret information, it is desirable to keep such devices from being reverse engineered. As an anti-RE technique, there are two types of obfuscation and camouflaging [2]. Obfuscation hides the functionality and implementation of a design by inserting additional gates into it. Camouflaging is a layout-level technique which hampers image processing-based extraction of a gate-level netlist from an IC.

This paper proposes the diffusion programmable device (DPD) architecture as a newly camouflaging technique. Logic functions using the DPD architecture can be programmed by assigning the N-type or P-type dopant to the active region extraneous to a transistor. Thus, the proposed technique requires no special process step in semiconductor manufacturing, and needs only modification of diffusion layers in order to change the logic function.

*Ritsumeikan University

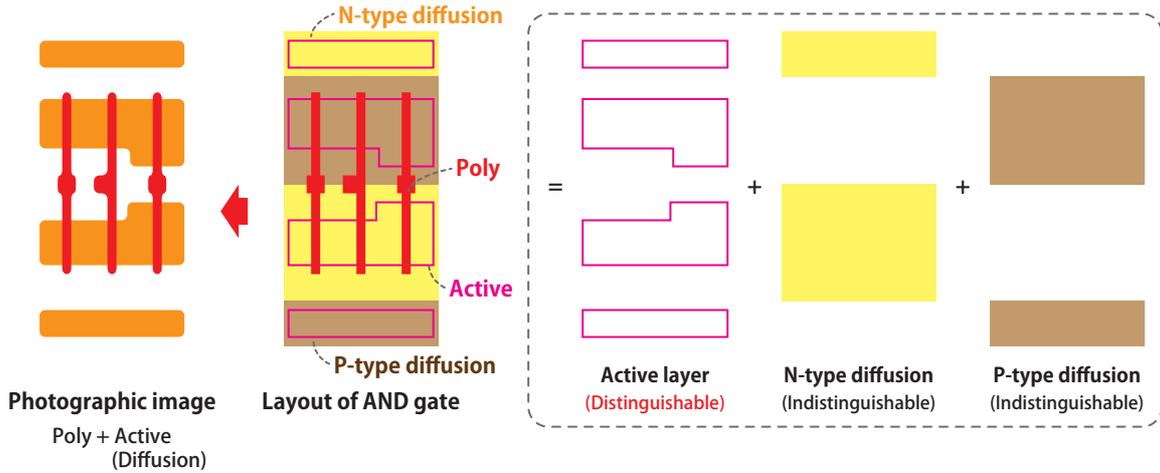


Figure 1: Reverse engineering in semiconductor.

2 Reverse Engineering and Countermeasures

The RE is misused to reveal the circuit structure of the device and estimate its functionality. At the RE in semiconductor, all the layers patterned during fabrication process are removed one-by-one in reverse order and the pattern layout is taken by the optical photograph. The attacker can re-construct the circuit by superposing the pattern layout in each layer.

The standard-cells used in typical ASIC has the specific metal pattern, then the circuit reconstruction can be achieved by analyzing only metal layers. In general, it is considered to be difficult to analyze the layers below metal layer using optical microscope, since the removal of all metal and via layers is time-consuming. Therefore some methods for anti-RE is proposed using the layers below the metal layers such as diffusion [4] [5] and well layers [6]. These methods make the attacker analyze all layers including silicon, gate poly, active, and well regions. However, since the shape difference of active regions (drain and source regions in a transistor) is distinguishable in principle, the countermeasure using the shape of the active layers [4] [5] may not be safe against RE attacks, as shown in Fig. 1. The countermeasure using well implants [6] requires special process step in semiconductor manufacturing.

3 Anti-RE Method using Doping Type Assignment

Our anti-RE technique can assign several different logic functions through dopant modification. This key element block is a diffusion programmable (DP) ROM cell which can be programmed to the output 1 or 0 by changing doping type (P-type or N-type) in the two active regions, as shown in Fig. 2. The logic value of ROMs can not be discriminated from the shape of active layer, since all the layout except diffusion layer is identical.

Next, the DPD Look-up-Table (LUT), whose function is programmed by the DP-ROMs, is shown in Fig. 3. The DPD-LUT is composed of three MUX gates and four DP-ROMs (S1-S4). When the logic XNOR operation is required, S1 and S4 are programmed to the output 1. Moreover, S2 and S3 are programmed to the output 0. In a similar way, all 2-input logic operations such as AND, OR, and XOR etc. can be configured by the DPD-LUT.

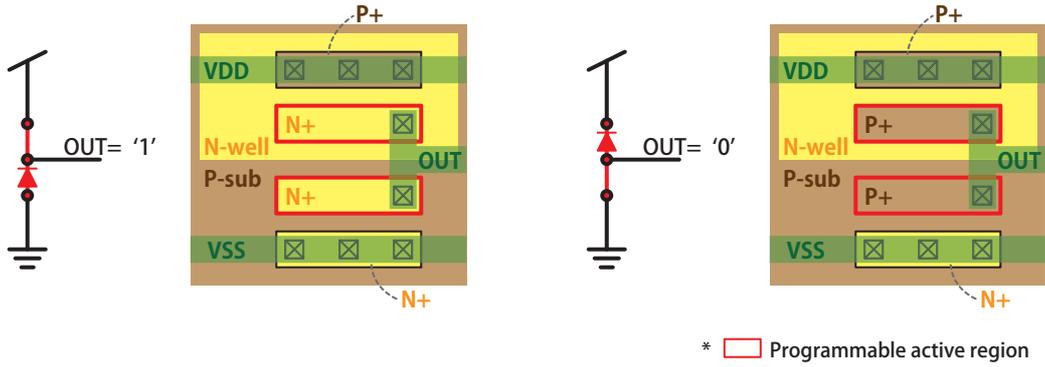


Figure 2: DP-ROM.

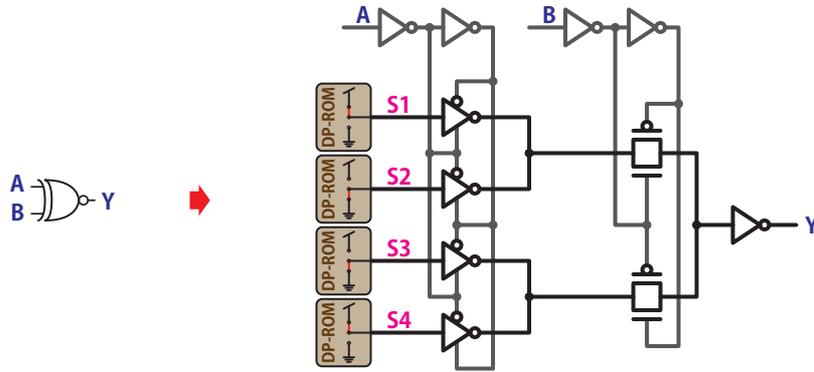


Figure 3: The DPD-LUT operated as a XNOR gate.

To verify the effectiveness of the proposed technique, a test element group (TEG) chip of the DPD-LUT was designed and fabricated with a 180nm CMOS technology. Fig. 4 shows layout of the DPD-LUT macro cell. The red rectangles indicate four DP-ROMs (S1-S4) of Fig. 3. The programmable active regions of S1 and S4 are assigned to N-type, and those of S2 and S3 are assigned to P-type to operate as the XNOR gate.

We made sure the logic gates (AND, OR, XOR, XNOR) using the DPD-LUT operated in the measurements. Fig. 5 shows output waveforms according to an input on the XNOR gate using the DPD-LUT. The result demonstrates that the logic gate using the DPD-LUT operates correctly.

4 Conclusions

In this paper, we proposed the newly anti-reverse engineering architecture termed the DPD. The DPD-LUT can configure all 2-input logic functions by changing the doping type to the programmable active regions. In addition, we designed and fabricated test chip using the DPD-LUT with a 180nm CMOS technology, and confirmed the correct logic operations on various gates. In the DPD-LUT architecture, 3 or 4-input LUT can be designed in the same manner. Therefore, all combinational circuit can be replaced by DPD-LUT, and the circuit will obtain the resiliency against RE. However, the chip area will be several times larger than that of original

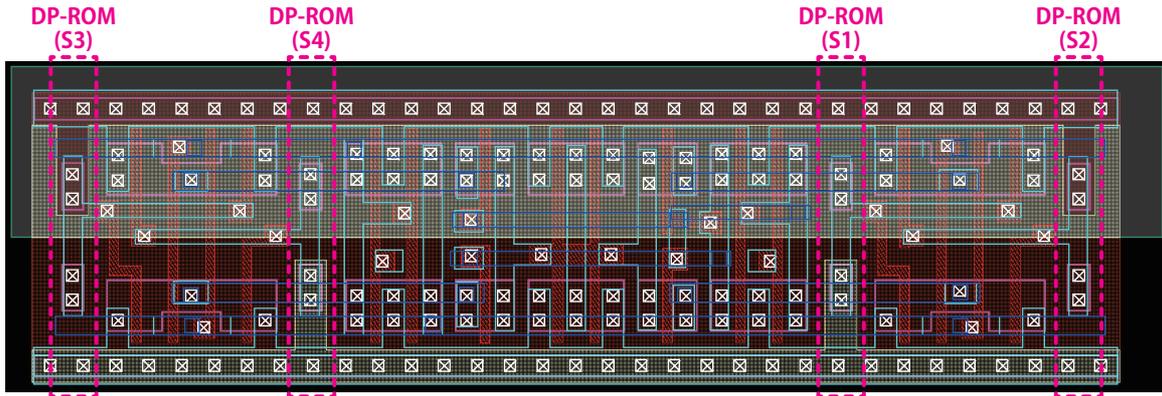


Figure 4: The layout of the DPD-LUT in a 180nm process.



Figure 5: The logic operation of the XNOR gate using the DPD-LUT.

one. The DPD-LUT logic cell can be used as a member of standard cell library, because the cell height of DPD-LUT is equal to that of standard cell. So, it is practically preferable that some portion of logic cells should be replaced to the DPD-LUT.

Acknowledgments

This research was supported by JST, CREST. The chip implementation was supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Rohm, Co., Ltd.

References

- [1] R. Torrance and D. James, "The state-of-the-art in semiconductor reverse engineering," Design Automation Conference (DAC), pp. 333 - 338, 2011.
- [2] M. Rostami, F. Koushanfar, J. Rajendran and R. Karri, "Hardware security: Threat models and metrics," Computer-Aided Design (ICCAD), pp. 819 - 823, 2013.

- [3] P. Subramanyan, N. Tsiskaridze, K. Pasricha, D. Reisman, A. Susnea and S. Malik, "Reverse Engineering Digital Circuits Using Functional Analysis," Design, Automation and Test (DATE), pp. 1277 - 1280, 2013.
- [4] James P. Baukus, William M. Clark, Jr., Lap-Wai Chow, and Allan R. Kramer, "Integrated circuit security system and method with implanted interconnections," US Patent No. 5866933, 1999.
- [5] James P. Baukus, William M. Clark, Jr., Lap-Wai Chow, and Allan R. Kramer, "Secure integrated circuit," US Patent No. 6294816, 2001.
- [6] Lap-Wai Chow, William M. Clark, Jr., James P. Baukus, and Gavin J. Harbison, "Integrated circuit modification using well implants," US Patent No. 8524553, 2013.