Reversing Stealthy Dopant-Level Circuits

Takeshi Sugawara[1], Daisuke Suzuki[1], Ryoichi Fujii[1], Shigeaki Tawa[1]
Ryohei Hori[2], Mitsuru Shiozaki[2], and Takeshi Fujino[2]

[1] Mitsubishi Electric Corporation
[2] Ritsumeikan University
sugawara.takeshi@bp.mitsubishielectric.co.jp

Abstract. A successful detection of the stealthy dopant-level circuit (trojan), proposed by Becker *et al.* at CHES 2013 [1], is reported. Contrary to an assumption made by Becker *et al.*, dopant types in active region are visible with either scanning electron microscopy (SEM) or focused ion beam (FIB) imaging. The successful measurement is explained by an LSI failure analysis technique called the passive voltage contrast [2]. The experiments are conducted by measuring a dedicated chip. The chip uses the diffusion programmable device [3]: an anti-reverse-engineering technique by the same principle as the stealthy dopant-level trojan. The chip is delayered down to the contact layer, and images are taken with (1) an optical microscope, (2) SEM, and (3) FIB. As a result, the four possible dopant-well combinations, namely (i) p+/n-well, (ii) p+/p-well, (iii) n+/n-well and (iv) n+/p-well are distinguishable in the SEM images. Partial but sufficient detection is also achieved with FIB. Although the stealthy dopant-level circuits are visible, however, they potentially make a detection harder. That is because the contact layer should be measured. We show that imaging the contact layer is at most 16-times expensive than that of a metal layer in terms of the number of images[3].

Keywords: Stealthy dopant-level trojan, Chip reverse engineering, LSI failure analysis, Passive voltage contrast

1 Introduction

Chips are widely used as "roots of trust" in modern security systems. The trust originates from properties that chip internals are difficult to inspect and/or modify. Limitations and improvements of such properties have been studied over the last decades in the chip security community. Recently, two related threats to the properties are drawing attentions. They are (i) hardware trojan and (ii) chip reverse engineering.

Hardware trojans are malicious modifications or implantations to circuit systems. An attacker uses a trojan as a backdoor to compromise security of a chip.

Threats of hardware trojans are emerging because of the globalization [1]. Nowadays, many parties (*e.g.*, IP vendors, design houses, foundries, assembly and testing companies, etc.) are commonly involved in a chip development. The parties are not always trustworthy.

In chip reverse engineering, on the other hand, an attacker tries to recover a netlist (or ultimately its logical functionality) of a target chip. The attempt is made by investigating depackaged and delayered chips. The attacker is motivated, for examples, (i) to make fakes, (ii) to obtain trade secrets, or (iii) to get an embedded secret key, etc. Nohl *et al.* showed a successful recovery of a hidden cipher algorithm as a result of reverse-engineering an RFID chip [4]. Analysis techniques are catching up with shrinking CMOS process. Torrance and James [5] showed that even a chip fabricated by a modern processes can be reverse-engineered.

Two problems are related. They can be modeled as a game between two players:

- *Hider* who try to hide something in a chip,
- *Seeker* who try to find the hidden something.

Note that the players *Hider* and *Seeker* appear throughout this paper. The labels are used because roles of an attacker and a defender are interchanged between the contexts of the hardware trojan and reverse engineering.

Seemingly, *Hider* is now advantageous because of the stealthy dopant-level trojans proposed by Becker *et al.* at CHES 2013 [1]. In the stealthy dopant-level trojan, dopant types in active region is modified. The proposers assume that measuring dopant types should be difficult even with scanning electron microscopy (SEM). If the assumption is true, then *Seeker* cannot find the trojan. Becker *et al.* showed a proof-of-concept modification and some realistic attack scenarios, which attracted much attentions [6]. Such a modification in active region is realistic especially when the trojan is implanted by a malicious foundry.

Soon after the proposal by Becker *et al.*, an anti-reverse-engineering technique called the diffusion programmable device (DPD) was proposed by Shiozaki *et al.* [3]. DPD uses the same principle as the stealthy dopant-level trojan. Therefore, reverse engineering of DPD is as difficult as detecting the stealthy dopant-level trojan. Both (i) the stealthy dopant-level trojan and (ii) DPD are referred to as "stealthy dopant-level circuits" in this paper.

As a first contribution, validity of the assumption, on which the stealthy dopant-level circuits are based, is examined with concrete experiments. Specifically, a dedicated chip containing DPD is measured with (a) an optical microscope, (b) SEM and (c) focused ion beam (FIB). As a result, we show that the stealthy dopant-level circuit is detectable contrary to the assumption made by the proposers. All the four possible dopant-well configurations, namely (i) p+/n-well, (ii) p+/p-well, (iii) n+/n-well and (iv) n+/p-well are distinguishable with SEM imaging. In addition, partial success is achieved with FIB imaging. The reason is explained by a technique called the passive voltage contrast (PVC) [2] studied in the LSI failure analysis community [5] [7] [8].

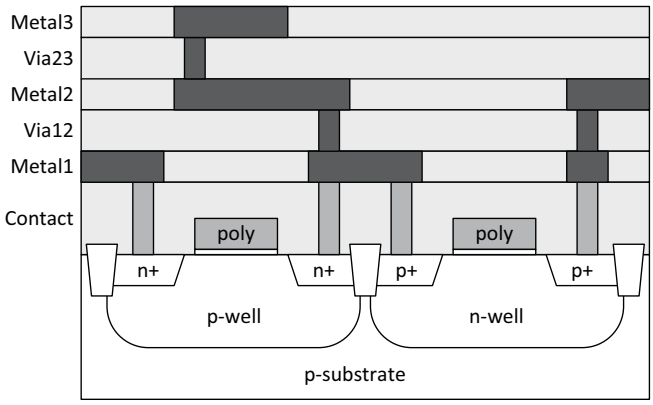

Fig. 1. Cross-sectional view of a CMOS circuit

Although the stealthy dopant-level circuits are visible, however, they potentially make the detection harder. That is because the contact layer should be measured for detection. As a second contribution, the cost is estimated in terms of the number of images. We show that imaging of the contact layer can be 16-times expensive than that of the first metal (M1) layer in our setup.

2 Stealthy Dopant-level Circuits

2.1 CMOS Circuit Fabrication

We firstly recall chip internals focusing on dopants. Fig. 1 shows a cross-sectional view of a common CMOS circuit. It has a layered structure. The layers are created through a series of processes summarized as [9]:

1. create n- and p-wells,
2. deposit and pattern polysilicon layer,
3. implant source and drain regions,
4. deposit and pattern metal layers.

Photo masks are used to determine shapes of circuits in the processes. A goal of circuit designers is to design layouts that is then converted to the photo masks.

In the stealthy dopant-level circuits, wells and dopants play important roles. At the process 1, wells are formed by implanting a moderate concentration of dopant on substrate. The implanted region is referred to as p- or n-wells depending on the types of dopants. Then, at the process 3, the source and drain junctions are formed by doping a high concentration of dopant (shown as n+ and p+) on the wells. Here, the p+/n+ regions are called active regions. Finally, contact plugs are formed. They connect between the p+/n+ regions and upper metal layers.

Notation There are four possible dopant-well combinations. They are denoted as (i) p+/p-well, (ii) p+/n-well, (iii) n+/p-well and (iv) n+/n-well in this paper. Corresponding dopant types are summarized in Tab. 1. Two different junctions: the Ohmic and PN junctions are formed. The Ohmic and PN junctions form a resistor and diode, respectively.

Table 1. Notation

name	source/drain dopant	well dopant	junction
(i) p+/p-well	p	p	Ohmic junction
(ii) p+/n-well	p	n	PN junction
(iii) n+/p-well	n	p	PN junction
(iv) n+/n-well	n	n	Ohmic junction

2.2 Stealthy Dopant-Level Trojans

Becker *et al.* proposed a new hardware trojan at CHES 2013 [1]. Their idea is to make a trojan just by modifying dopant types in active region. They showed a proof-of-concept circuit modification to a CMOS inverter. If the modification is made, an output of the inverter is stuck to a constant.

Mechanism behind the modification is explained. Fig. 2 (1) shows an original CMOS inverter. Fig. 2 (2), (3) are modified ones. When the modification shown in Fig. 2 (2) is made, the output port Y is tied to V_{DD} through a resistor formed by the n+/n-well. The connection between the port Y and GND is opened because of a diode formed by n+/p-well. Therefore, V_{DD} and GND are safely insulated. As a result, the output of the inverter is always high, *i.e.*, it is stuck at 1. Stuck-at-0 fault is achieved by an alternative modification shown in Fig. 2 (3).

Such a simple principle leads a variety of applications. Becker *et al.* showed example attack cases targeting (i) Intel Ivy Bridge RNG and (ii) iMDPL: a gate-level side-channel attack countermeasure.

An attempt to detect the trojan is made as follows [1] [11]. Firstly, a target chip is depackaged and a bare chip is exposed. Then, the bare chip is delayered one by one through polishing or etching [4] [5]. The exposed layers are measured with an imager *e.g.*, SEM. Secondly, the images are compared with golden images for a possible difference [1]. Becker *et al.* assume that distinguishing dopant types in such images is difficult. Consequently, the trojan made by the dopant-type modification should be undetectable.

2.3 DPD: Diffusion Programmable Device

DPD is an anti-reverse-engineering technique inspired by the stealthy dopant-level trojan [3]. The idea is to make a programmable look-up table (LUT), similar to that of an FPGA, but programmed by dopant (cf. SRAM in FPGA). There

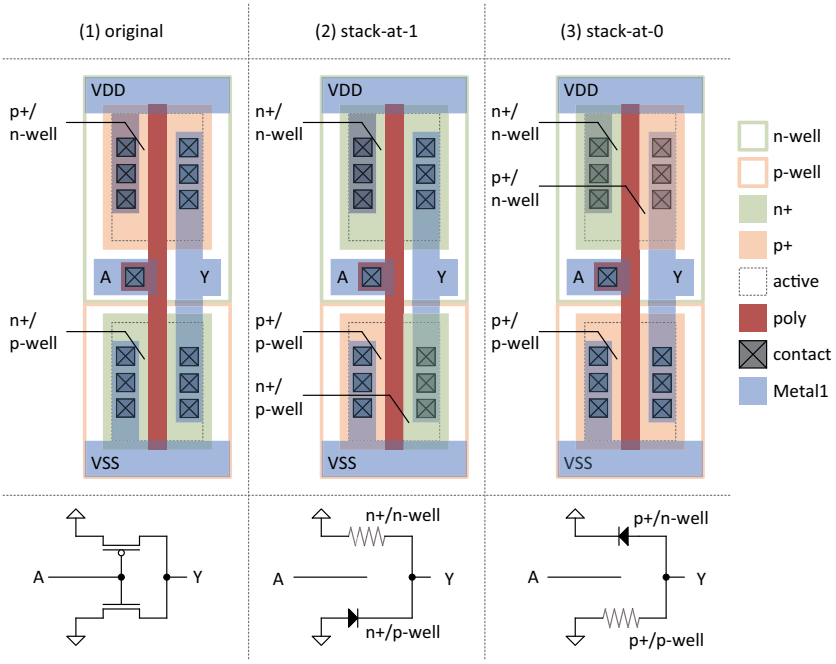

Fig. 2. Stealthy dopant trojan

was a conventional dopant-based anti-reverse-engineering technique [11] [12] on which the work by Becker *et al.* is based. However, DPD is the first academic publication on the topic to the best of our knowledge.

Fig. 3 depicts a schematic diagram of a design unit called the DPD logic element (DPD-LE). DPD-LE implements a 2-input LUT. The two inputs A and B are used to select one out of four terminals. The terminals $S_1, \cdots, S_4$ are connected to the dopant-programmed ROM. The ROM is made with the stuck-at-0 and stuck-at-1 modifications shown in Fig. 2. Note that for the sake of performance, the ROM in DPD-LE is simplified from the ones shown in Fig. 2. DPD-LE can be configured to any 2-input gate. Tab. 2 shows a truth table of example configurations.

Layout of the DPD-LE is shown in Fig. 4 where programmable regions are indicated with rectangles. Similar to the stealthy dopant-level trojan, logic functions using DPD-LE are identical except for dopant types in the programmable regions.

An attempt of reverse-engineering is conducted as follows. Chip images are taken in the same manner as the trojan detection. Then, the images are analyzed with an image-processing tool [10] to extract standard cells and interconnections [10]. To reverse-engineer a circuit with DPD, *Seeker* needs revealing the ROM contents $S_1, \cdots, S_4$. However, that is as difficult as finding the stealthy-dopant trojan. Therefore, *Seeker* cannot recover a netlist from the images.

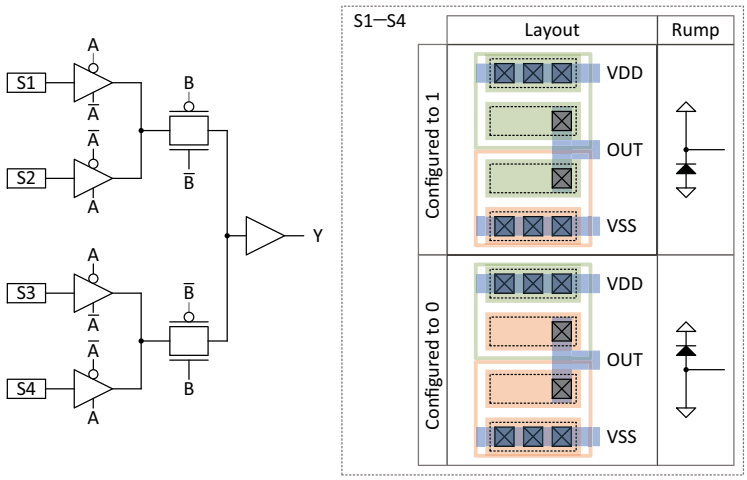

Fig. 3. Schematic of the DPD-LE

Table 2. Truth table of DPD-LE

A	B	XOR	XNOR	BUF_B	INV_B	BUF_A	INV_A	OR	NOR	AND	NAND
0	0	S_1=0	S_1=1	S_1=0	S_1=1	S_1=0	S_1=1	S_1=0	S_1=1	S_1=0	S_1=1
0	1	S_2=1	S_2=0	S_2=1	S_2=0	S_2=0	S_2=1	S_2=1	S_2=0	S_2=0	S_2=1
1	0	S_3=1	S_3=0	S_3=0	S_3=1	S_3=1	S_3=0	S_3=1	S_3=0	S_3=0	S_3=1
1	1	S_4=0	S_4=1	S_4=1	S_4=0	S_4=1	S_4=0	S_4=1	S_4=0	S_4=1	S_4=0

3 Measurement Principle

In this section, we firstly recall a measurement principle of SEM and FIB. Then, we explain a measurement technique called PVC [2] which potentially detects dopant types.

3.1 Measurement using SEM/FIB

SEM is a common instrument for LSI failure analysis. FIB is another popular instrument for the same purpose. Although FIB is known for circuit modification (*e.g.*, micro surgery) [7], however, it can also be used as an imager based on the same principle as SEM.

SEM and FIB are advantageous in spatial resolution over optical microscopy. Resolution of optical microscopy is restricted by wave lengths of lights that are around 200 nm. That correspond to around 250–180 nm CMOS processes [4]. Therefore, SEM or FIB is indispensable for imaging chips fabricated with modern CMOS processes.

A measurement system of SEM/FIB is shown in Fig. 5. Measurement is conducted as follows:

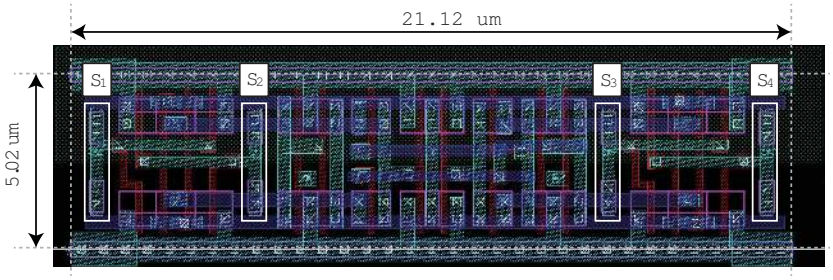

Fig. 4. Layout of DPD-LE configured to XOR

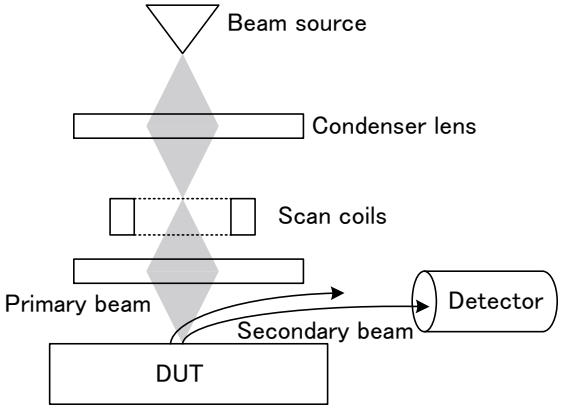

Fig. 5. SEM/FIB measurement system

1. A primary beam (*i.e.*, accelerated electrons or ions) is injected onto sample surface.
2. As reaction to the primary beam, secondary electrons are emitted from the surface of the sample.
3. The number of secondary electrons is measured at the detector.
4. Iterate the above measurement by scanning the primary beam through magnetic field in the coils. Finally, a contrast image is complete.

The primary beam is different between SEM and FIB; electron and ions are used, respectively.

3.2 PVC: Passive Voltage Contrast

SEM/FIB can also be used to measure surface voltage of a sample. That is because a static field formed by the surface voltage interferes with secondary electrons. As a result, the number of secondary electrons caught at the detector is changed. Measurement based on the principle is called PVC. The method was developed in 90s and now widely used. We refer a paper by Rosenkranz as a

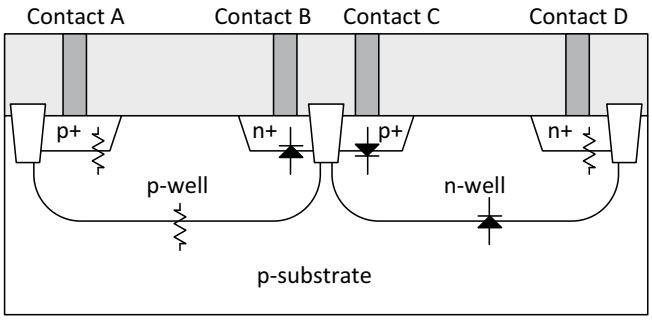

Fig. 6. Contacts and different dopant-well configurations

good survey on the topic [2]. Voltage-contrast images of DRAM and SRAM are found in the paper by Rosenkranz [2] and one by Chen *et al.* [13], respectively.

The dopant configurations in Tab. 1 can be distinguished with PVC even when a chip is measured at power-off state. In the following description, we consider a case wherein contact plugs in Fig. 6 are measured with SEM.

When the primary beam is accelerated by a voltage around 0.7 kV, the total number of secondary electrons emitted from the plug exceeds that of the injected primary electrons. As a result, the plug charges positively by lack of electrons. At the same time, external electrons are provided to the plug because of the voltage difference. In other words, the positive charges are shared by a whole conductive region from the plug. A resulting surface voltage, at stationary state, is determined by the mass of the region conducted to the contact plug. The mass depends on a dopant-well configuration. That attributes to diodes formed by PN junctions as shown in Fig. 6. For example, the contact B has the smallest conductive region (*i.e.*, the n+ region only) because of a reverse PN junction illustrated as a diode. On the other hand, the contact A has the largest conductive region involving the p-well, n-well, and p-substrate. As a result, the masses of the conductive regions are ordered as the contacts A $>$ C $\approx$ D $>$ B. When the resulting surface voltages are compared, they are ordered as the contacts A $<$ D $<$ C $<$ B. Note that the difference between the contacts C and D is caused by the diffusion potential at the p+/n-well.

When the plug charges positively, secondary electrons are attracted back to the plug, and thus less is measured at the detector. Therefore, brightness of a corresponding pixel in a SEM image become darker as the plug voltage is higher (conversely, it become brighter as the voltage is lower). As a result, the brightnesses of the plugs are ordered as A $>$ D $>$ C $>$ B, or equivalently (i) p+/p-well $>$ (iv) n+/n-well $>$ (ii) p+/n-well $>$ (iii) n+/p-well. As a result, the configurations (i)–(iv) in Tab. 1 can be distinguished by looking at contacts in SEM images.

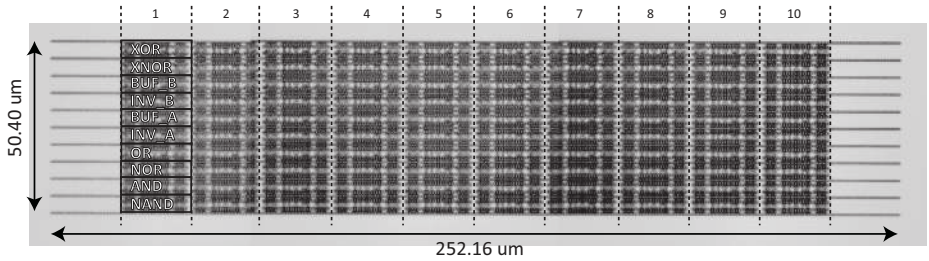

Fig. 7. An optical microscopy image of the DPD array in a delayered chip

4 Experiment

4.1 Target Chip

Experiments are conducted using a chip implementing DPD. The chip is fabricated using the Rohm 180-nm CMOS process[4]. As a preparation, upper layers of the chip are removed with mechanical polishing and the contact layer is exposed.

Fig. 7 shows an optical-microscopy image of the prepared chip. The figure shows a DPD array containing 10×10 DPD-LEs configured to different 2-input logic gates. That are XOR, XNOR, BUF_B, INV_B, BUF_A, INV_A, OR, NOR, AND, and NAND gates as shown in Fig. 7.

4.2 Experiment 1: Distinguishing Dopant Types

The prepared chip is measured with SEM and FIB. We used the Hitachi High-Technologies S-5200 SEM and FB-2100 FIB.

DPD-LE configured to 2-input XOR is measured. Results are shown in Fig. 8. Fig. 8 (1) is the original layout. Regions shown in green and yellow correspond to $S_1, \cdots, S_4$ where $(S_1, S_2, S_3, S_4) = (0, 1, 1, 0)$. Fig. 8 (2), (3), (4) are images taken with (2) an optical microscope, (3) SEM, and (4) FIB. Many dots found in the images are contact plugs. The rectangles indicate the programmable regions (see Fig. 4).

Dopant types are undetectable by optical microscopy as shown in Fig. 8 (2). Meanwhile the contacts show different brightnesses in SEM/FIB images in Fig 8 (2) and (3). In the SEM image shown in Fig 8 (3), the brightnesses of the contacts are (p+/p-well, p+/n-well, n+/p-well, n+/n-well) = (white, dark grey, black, light grey), as expected in Sect. 3.2. Therefore, the four possible configurations are distinguishable. In the FIB image shown in Fig. 8 (4), on the other hand, (p+/p-well, p+/n-well, n+/p-well, n+/n-well) = (white, white, black, white). Only the n+/p-well is distinguishable from others with FIB.

[4] We used the 180-nm process because a good fabrication service is available. That does not mean PVC works only with old processes; PVC works with recent processes. For example, a successful PVC of a 65-nm SRAM is reported [15].

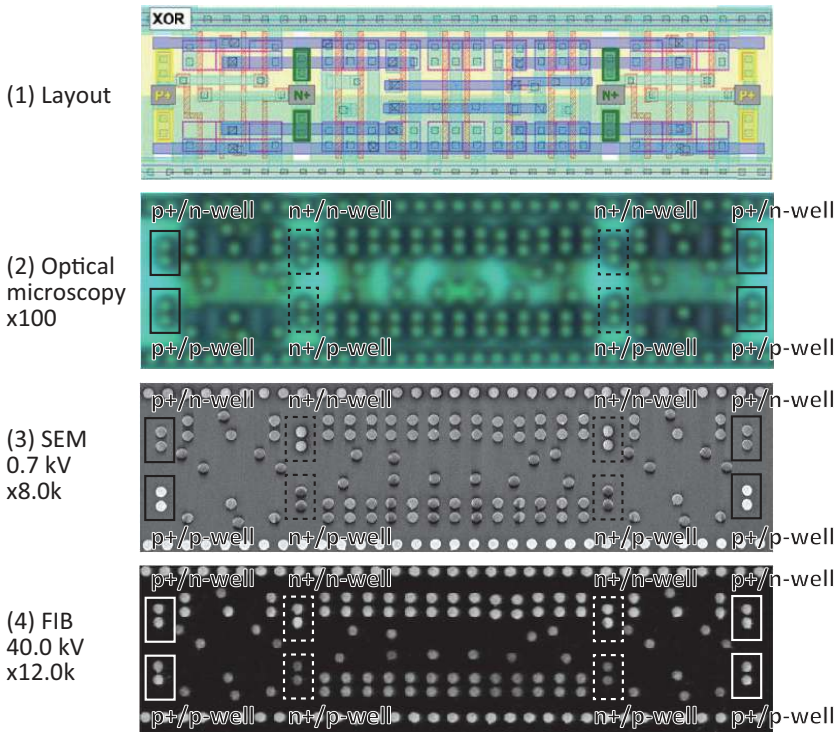

Fig. 8. Image of DPD-LE configured as XOR

The same experiment is repeated for other DPD-LEs configured to other logic gates. Results are shown in Fig. 9. We can observe different brightnesses depending on S_1–S_4 configurations. That correspond to the ROM contents (S_1, S_2, S_3, S_4) summarized in Tab. 2. The results also indicate that measurements are well reproducible.

4.3 Experiment 2: Distinguishing Dopant Types under Various Measurement Conditions

The stealthy dopant-level circuits are visible. However, they potentially make a detection harder. That is because the contact layer should be measured in addition to metal layers. One metric to evaluate the cost of detection is the number of images. That is because (i) usage of an instrument (e.g., SEM) is sometimes charged at an hour each [16], and (ii) a computational cost to process acquired images should depend on data size[5]. The relationship between the (i) number of images and (ii) gate counts are estimated in Appendix.

[5] The cost to recover a netlist is not considered. That is an emerging research topic and is beyond the scope of this paper.

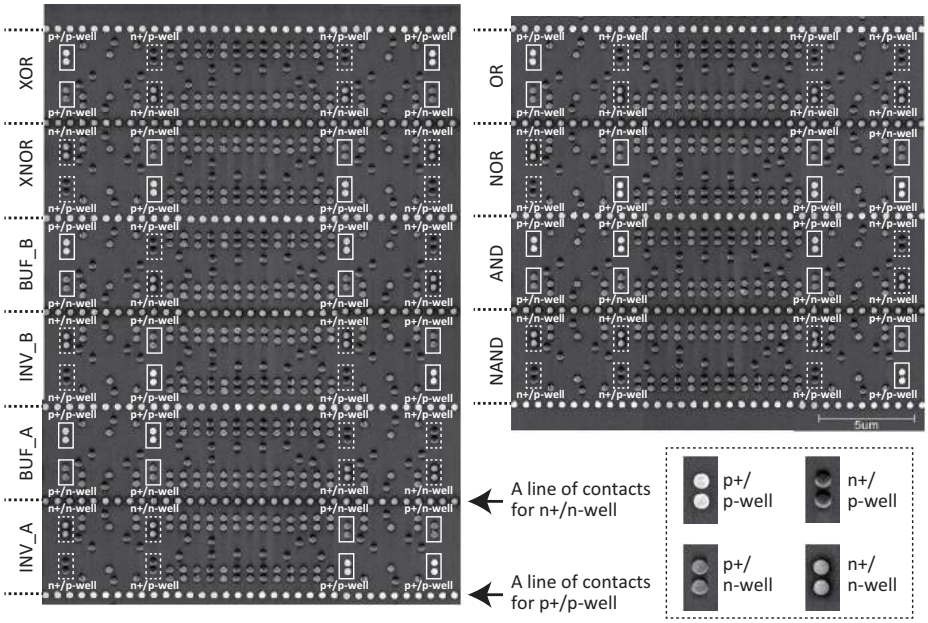

Fig. 9. SEM images of DPD-LE with various configurations

In order to estimate the cost, the chip is measured with different configurations: (i) acceleration voltage, (ii) scan speed, and (iii) magnification. Tab. 3 summarizes examined configurations and corresponding brightnesses of contacts. The acquired images are shown in Fig. 10.

Firstly, difficulty to detect non-dopant patterns is discussed. It is a common practice to use patterns in the M1 layer to identify types of standard cells [10] [14]. Therefore, the layer is desirable as a counterpart. Images Fig. 10 (2) and (3) are SEM images acquired at magnifications of x400 and x1.5k, respectively. The contacts are not visible in Fig. 10 (2). Therefore, the magnification of x1.5 is needed to image contacts. Patterns in the M1 layer, that lead standard-cell identifications, are in the similar dimension as contacts [14]. Therefore, we assume that the limit of magnification to measure the M1 layer is x1.5k in the following discussion.

If we want to distinguish the four dopant-well configurations, the case (5) in Tab. 3 is the only option. In that case, magnification should be at least x6.0k. Therefore, the number of images is 16 ($= (6.0k/1.5k)^2$) times larger than that of the M1 layer. In summary, the additional cost for *Seeker* to find the stealthy dopant-level circuits is the cost of imaging of one additional layer (*i.e.*, the contact layer). The layer is 16-times costly compared to the M1 layer.

On the other hand, distinguishing the four configurations is not necessary when the modifications in Fig. 2 are considered. That is because the dopant-well configurations appear in pairs. In other words, we can recover $S_1, \cdots, S_4$

Table 3. Visibility of dopants with different measurement configurations

Case	Inst.	Accele.	Scan	Magnification	(i) p+/p-well	(ii) p+/n-well	(iii) n+/p-well	(iv) n+/n-well
(1)	SEM	0.7 kV	Fast	x1.5k, x3.0k	White	Grey	Grey	Grey
(2)	SEM	0.7 kV	Slow	x100, x400,	—	—	—	—
(3)	SEM	0.7 kV	Slow	x1.5k	Black	White	Black	Black
(4)	SEM	0.7 kV	Slow	x3.0k	Grey	Grey	Grey	Grey
(5)	SEM	0.7 kV	Slow	x6.0k, x8.0k, x10.0k, x15.0k, x30.0k	White	Grey (dark)	Black	Grey (bright)
(6)	SEM	2.0 kV	Slow	x1.5k, x3.0k, x8.0k, x15.0k,	Grey	White	Grey	Grey
(7)	SEM	5.0 kV	Slow	x8.0k	Grey	White	Grey	Grey
(8)	SEM	30.0 kV	Slow	x8.0k	Grey	Grey	Grey	Grey
(9)	FIB	40.0 kV	Slow	x2.5k, x5.0k, x12.0k, x25.0k	White	White	Black	White

if one out of the four dopant-well configurations is distinct from others. Such a detection succeeds in the cases (1), (3), (5), (6), (7), and (9). Therefore, the x1.5k magnification is sufficient. That is the same as the one required for the M1 layer. As a result, the additional cost for detecting these circuits are very limited i.e., the costs for imaging the contact layer at the same magnification as the M1 layer.

Finally, we discuss how to determine dopant-well configurations given images only. That is not trivial because the relationship between brightnesses and the dopant-well configurations is not consistent as shown in Tab. 3. One possible solution is to conduct a profiling using an open sample fabricated with the same CMOS process. Even without open samples, we can make an educated guess. That is because references are found everywhere in the chip. Important landmarks are the lines of contacts marked in Fig. 9. They are used to tie p/n-well voltages to V_{DD}/GND, thus they should be p+/p-well and n+/n-well. Since wells are regularly placed, contacts near the line of p+/p-well contacts should be either p+/p-well or n+/p-well. In that way, *Seeker* can efficiently find reference contacts for the four dopant-well configurations. Such a guess become easier if standard cells are found in the chip.

5 Conclusion

The assumption behind the stealthy dopant-level circuits (i.e., the stealthy dopant-level trojan and the diffusion programmable device) is examined with concrete experiments. As a result, it is shown that all the four possible dopant-well combinations are distinguishable with SEM. It is also shown that the stealthy dopant-level circuits are resistant against optical microscopy, however, that mean only a limited practical benefit because modern CMOS circuits are small beyond the

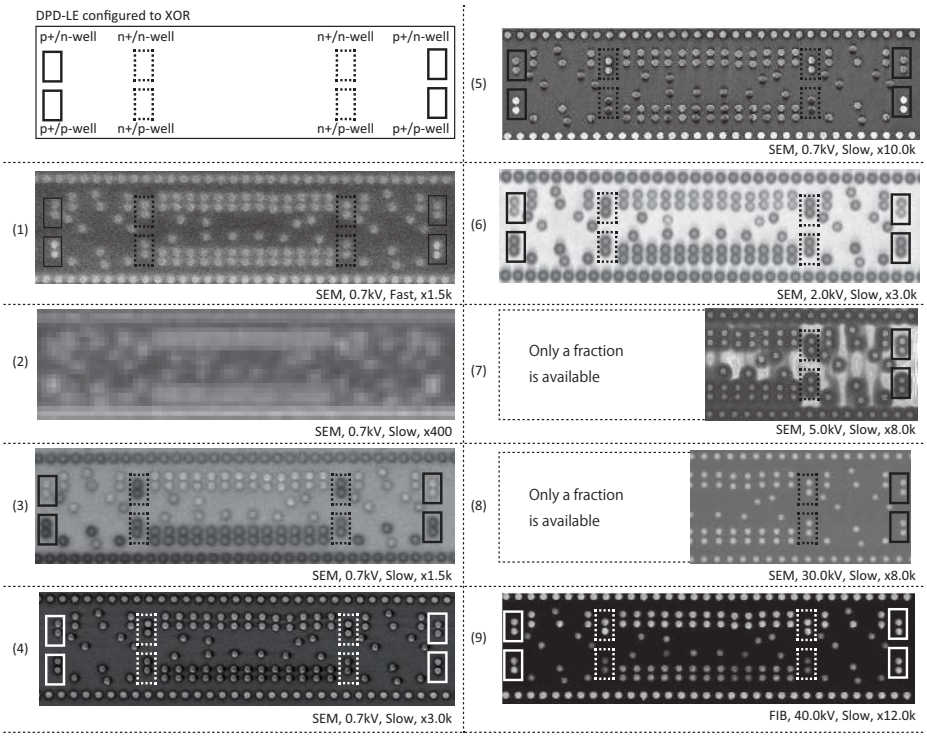

Fig. 10. Images with different configurations (the image numbers correspond to ones in Tab. 3)

limit of optical microscopy. To detect the stealthy dopant-level circuits, the contact layer should be measured. Additional experiments revealed that the layer can be 16-times more costly compared to the M1 layer in terms of the number of images. The results show that the assumption used in the previous works – dopant types are difficult to measure – was too optimistic.

An improved stealthy dopant-level circuit is opened for research. Since the measurement principle is known, thus we can possibly make a circuit that is invisible to the measurement. For example, the high contrast at p+/p-well could be reduced if p-well is isolated from substrate by a deep n-well that is available in a triple-well process. Meanwhile, the principle hints that a dopant modification is undetectable by PVC if modifications are limited to regions not connected to contact plugs. Making a meaningful circuit with the restriction is an interesting challenge. However, we stress that PVC is just one of many measurement techniques. Other options involve the active voltage contrast method and PVC combined with FIB circuit modifications [2]. Therefore, it would be more important to make a reasonable assumption considering these techniques, before rushing into studies of improved circuits/trojans. Knowledge in the LSI fail-

ure analysis community will help, because we will need to know state-of-the-art measurement techniques to make a reasonable assumption.

From the view point of trojan detection, cost will be a matter. That is because the detection becomes more expensive as chip size increases. It is estimated that we need 5.16 shots/kGE (see Appendix), but mega-gate chips are common now. One possible direction for settling the problem is to use a built-in testing instrument. The problem of finding a trojan in a chip may be reduced to a smaller problem of finding one in the testing instrument. However, Becker *et al.* already showed an example of bypassing a BIST (Built-in Self Test) without modifying the BIST itself. Building a sophisticated testing instrument will be an interesting research direction.

Another important viewpoint is a dilemma between goals of trojan detection and anti reverse engineering. We want *Hider* to win the game in reverse engineering and *Seeker* to win in trojan detection at the same time. A problem of finding a new technique that satisfies both requirements is opened. An important observation is that there are asymmetric capabilities between trojan attackers and circuit engineers. For example, the circuit engineers are allowed to modify metal layers while the (dopant-level) trojan attackers are not.

Acknowledgement

The authors would like to thank the anonymous reviewers at CHES 2014 for their valuable comments. The study was conducted as a part of the CREST Dependable VLSI Systems Project funded by the Japan Science and Technology Agency. The chip used in the paper was made in a fabrication program of the VLSI Design and Education Center at the University of Tokyo in collaboration with Rohm Corporation and Toppan Printing Corporation. The standard cell library used in the appendix was developed by the Tamaru and Onodera Laboratory at Kyoto University and released by the Kobayashi Laboratory at the Kyoto Institute of Technology.

References

1. G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy Dopant-Level Hardware Trojans", CHES2013, LNCS Vol. 8086, 2013, pp 197-214.
2. R. Rosenkranz, "Failure Localization with Active and Passive Voltage Contrast in FIB and SEM", Journal of Materials Science: Materials in Electronics, Vol. 22, Issue 10, pp. 1523–1535, October 2011.
3. M. Shiozaki, R. Hori, and T. Fujino, "Diffusion Programmable Device: The Device to Prevent Reverse Engineering", IACR Cryptology ePrint Archive 2014/109, 2014.
4. K. Nohl, D. Evans, Starbug, and H. Plötz, "Reverse-Engineering a Cryptographic RFID Tag", Proceedings of the 17th USENIX Security Symposium, 2008.
5. R. Torrance and D. James, "The State-of-the-Art in IC Reverse Engineering", CHES 2009, LNCS Vol. 5747 pp. 363–381, 2009.
6. Slashdot, "Stealthy Dopant-Level Hardware Trojans", `http://hardware.slashdot.org/story/13/09/13/1228216/stealthy-dopant-level-hardware-trojans`.

7. C. Tarnovsky, "(In)security of Commonly Found Smart Cards", Invited Talk II, CHES 2012.
8. C. Boit, "Security Risks Posed by Modern IC Debug and Diagnosis Tools", Keynote Talk I, 10th Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2013), 2013.
9. S. M. Kang and Y. Leblebici, "CMOS Digital Integrated Circuits Analysis & Design", McGraw-Hill, 2002.
10. Reverse engineering integrated circuits with degate, `http://www.degate.org/`.
11. J. Rajendran, M. Sam, O. Sinanoglu, and R. Karri, "Security Analysis of Integrated Circuit Camouflaging", 2013 ACM SIGSAC conference on Computer & communications security, pp. 709-720.
12. SypherMedia International. Circuit Camouflage Technology - SMI IP Protection and Anti-Tamper Technologies. White Paper Version 1.9.8j, March 2012.
13. H. Chen, R. Fan, H. Lou, M. Kuo, and Y. Huang, "Mechanism and Application of NMOS Leakage with Intra-Well Isolation Breakdown by Voltage Contrast Detection", Journal of semiconductor technology and science, vol.13, no.4, pp. 402–409, 2013.
14. Silicon zoo, Megamos chip XOR gate, `http://www.siliconzoo.org/megamos.html`.
15. M. Yang, S. Liang, L. Wu, L. Lai, J. Su, C. Niou, Y. Wen, Y. Zhu, "Application of Passive Voltage Contrast Fault Isolation on 65nm SRAM Single Bit Failure", 16th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits, 2009.
16. Electron Microscope Lab. at UC Berkeley, "Charges for training and use of EML facilities (11/2013)", `http://em-lab.berkeley.edu/EML/charge.php`.
17. Cryptographic Hardware Project at Tohoku Univ., Aoki Lab., `http://www.aoki.ecei.tohoku.ac.jp/crypto/web/cores.html`.

Appendix: Estimating the Number of Images per Gate

The relationship between (i) the number of gate elements, (ii) chip area, and (iii) the number of images is estimated.

As a target, we use an open-source AES core called `AES_Comp` [17]. The core is synthesized with the standard-cell library for the Rohm 180-nm process. The total cell area is 288,000 μm^2. The area corresponds to about 15 kGE. The utilization ratio after place and route is assumed to be 70 %. Then, the AES core uses about 411,000 μm^2 (=288,000/0.7).

In SEM imaging with x1.5k magnification, an area involved in a single image is about 5,000 μm^2 ($\approx$ 63 μm $\times$ 84 μm). Therefore, we need about 77 ($\approx$ 411,000/5,000) shots to cover the AES core. If we normalize the number of shots by the gate counts, we get 5.16 shots/kGE.