MITSUBISHI ELECTRIC
Changes for the Better

CHES 2014, 2014/Sep./24

Reversing Stealthy Dopant-Level Circuits

Takeshi Sugawara*

joint work with
Daisuke Suzuki*, Ryoichi Fujii*, Shigeaki Tawa*,
Ryohei Hori**, Mitsuru Shiozaki**, and Takeshi Fujino**

*Mitsubishi Electric Corp. and **Ritsumeikan Univ.

The study was conducted as a part of the CREST Dependable VLSI Systems Project funded by the Japan Science and Technology Agency

MITSUBISHI ELECTRIC
Changes for the Better

Quick overview

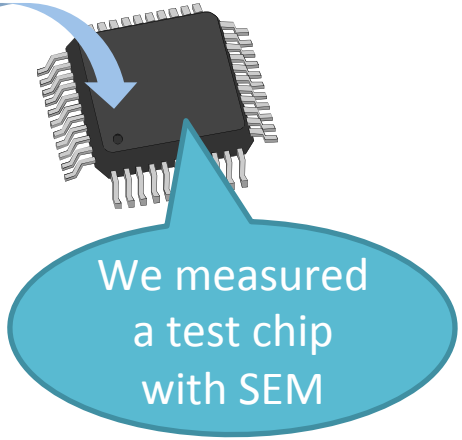
- Stealthy dopant-level circuits are visible contrary to an assumption

Dopant-level trojan
Becker et al.
(CHES 2013)

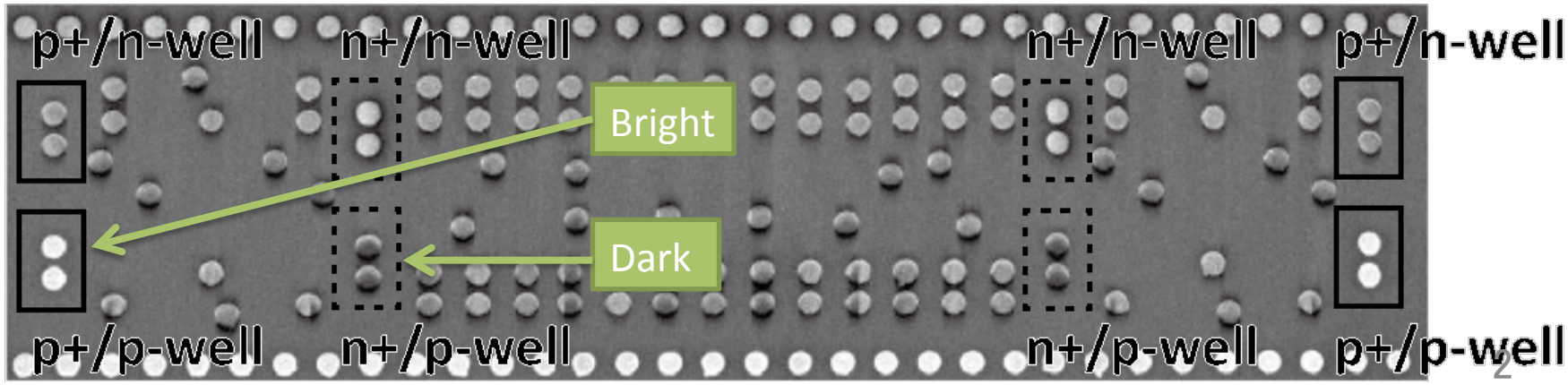
Make undetectable trojans by modifying dopants

Dopant-programmable device
Shiozaki et al. (eprint 2014)

Anti reverse engineering technique by the same principle. Proved in silicon.

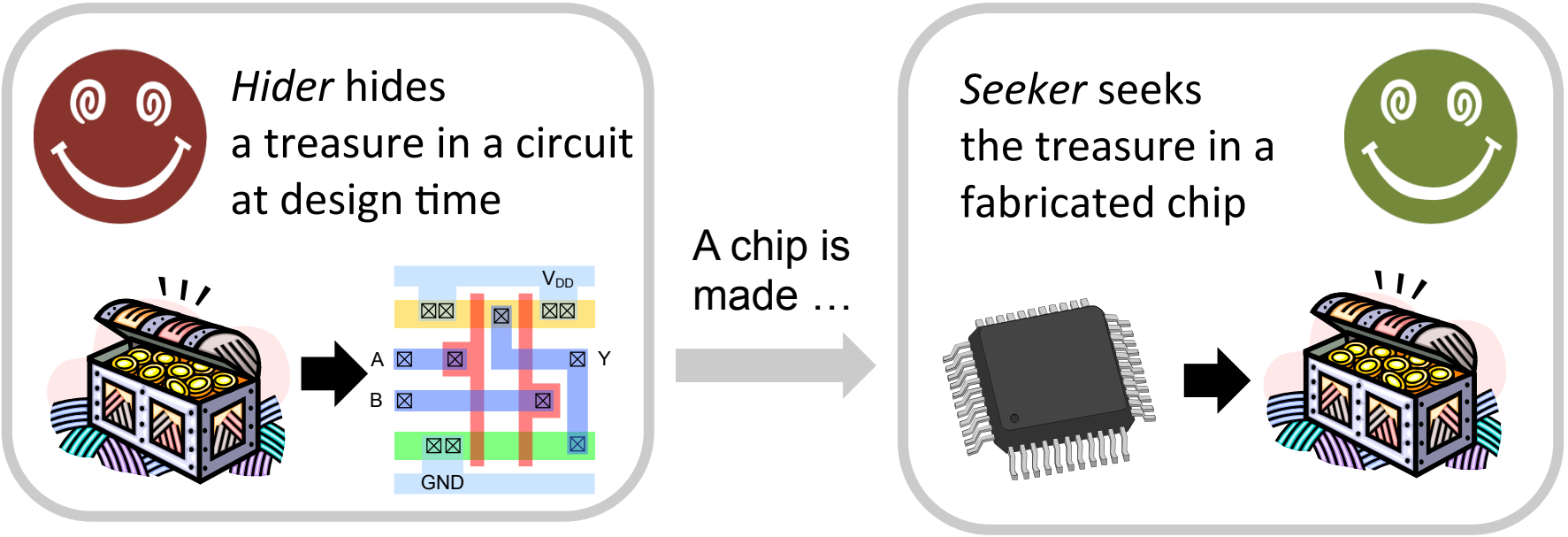


A SEM image of the test chip at the contact layer:
brightness differences between the dots mean the stealthy circuits are detectable



Duality: trojan detection and anti reverse engineering

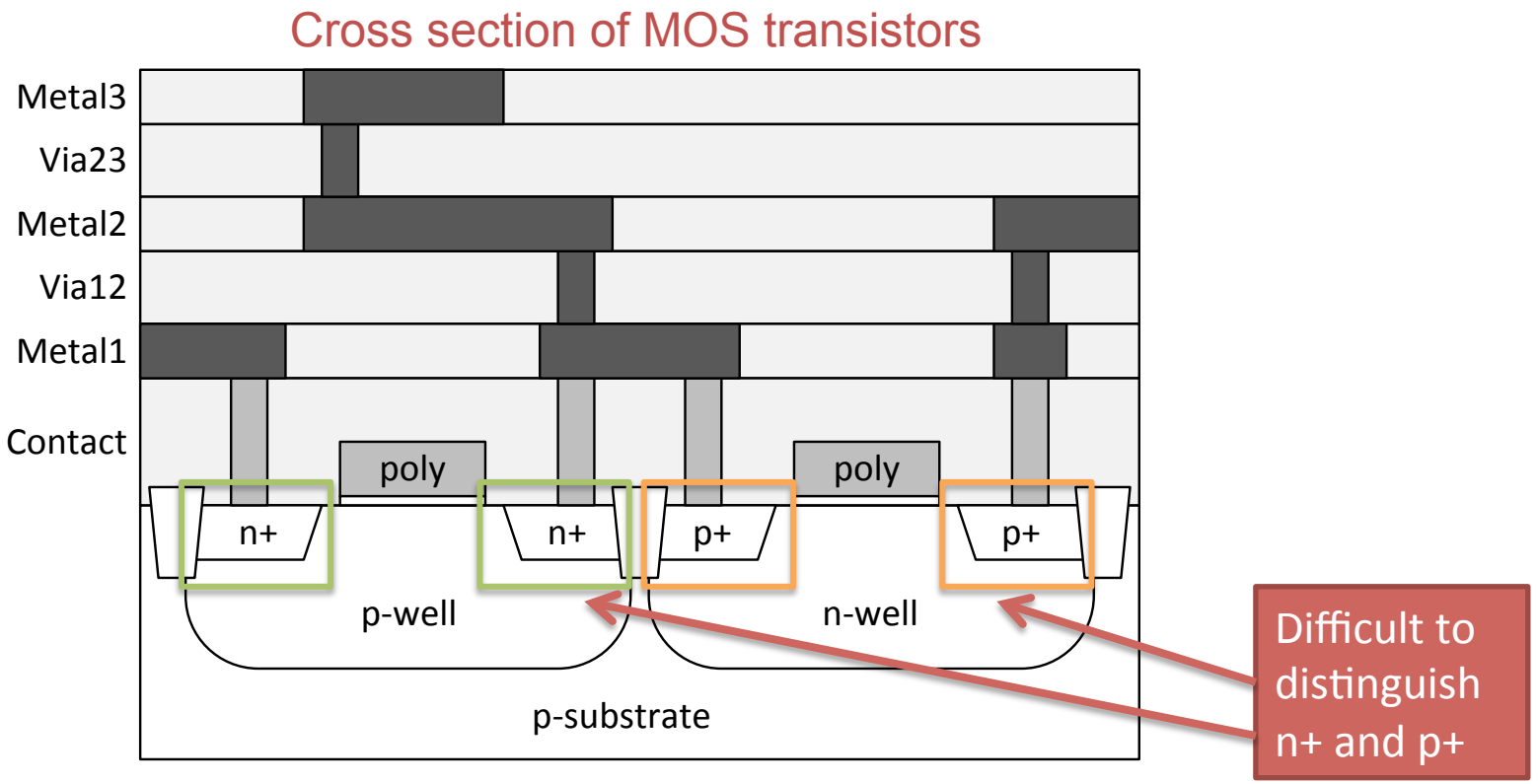
- A game between *Hider* and *Seeker*



- In trojan detection,
  - Treasure = trojan, *Hider* = attacker, *Seeker* = chip vendor
- In anti reverse engineering,
  - Treasure = proprietary circuit, *Hider* = circuit designer, *Seeker* = reverse engineer
- The dopant-level circuits make *Hider* advantageous

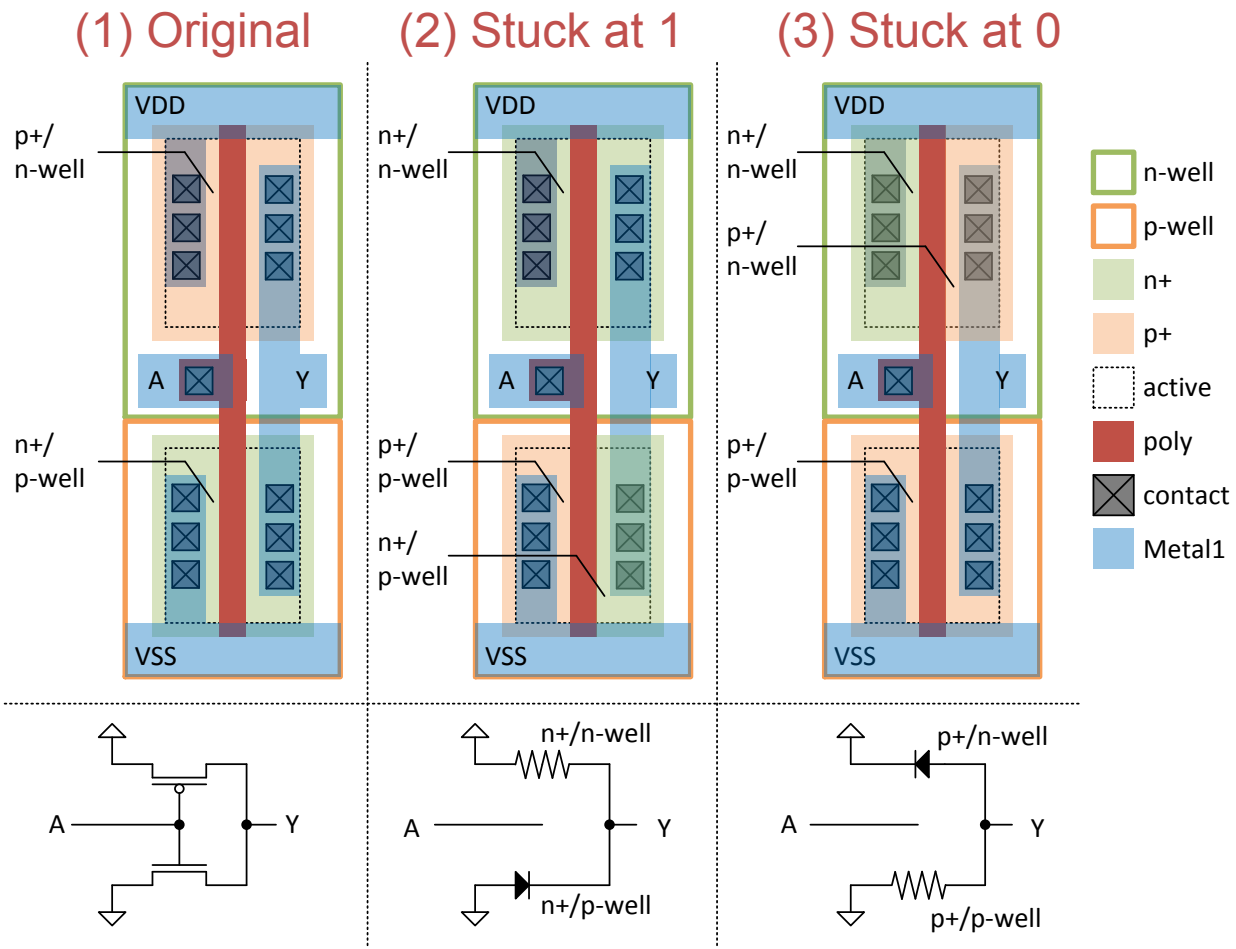
Stealthy Dopant-Level Circuits

- Undetectable circuits made by changing dopant types only
- Assumption: types of dopants are indistinguishable with visual inspection
  - Pro: the dopants are sparse; one dopant atom in $2^{42.185}$ silicon atoms
  - Correctness of the assumption was remained open



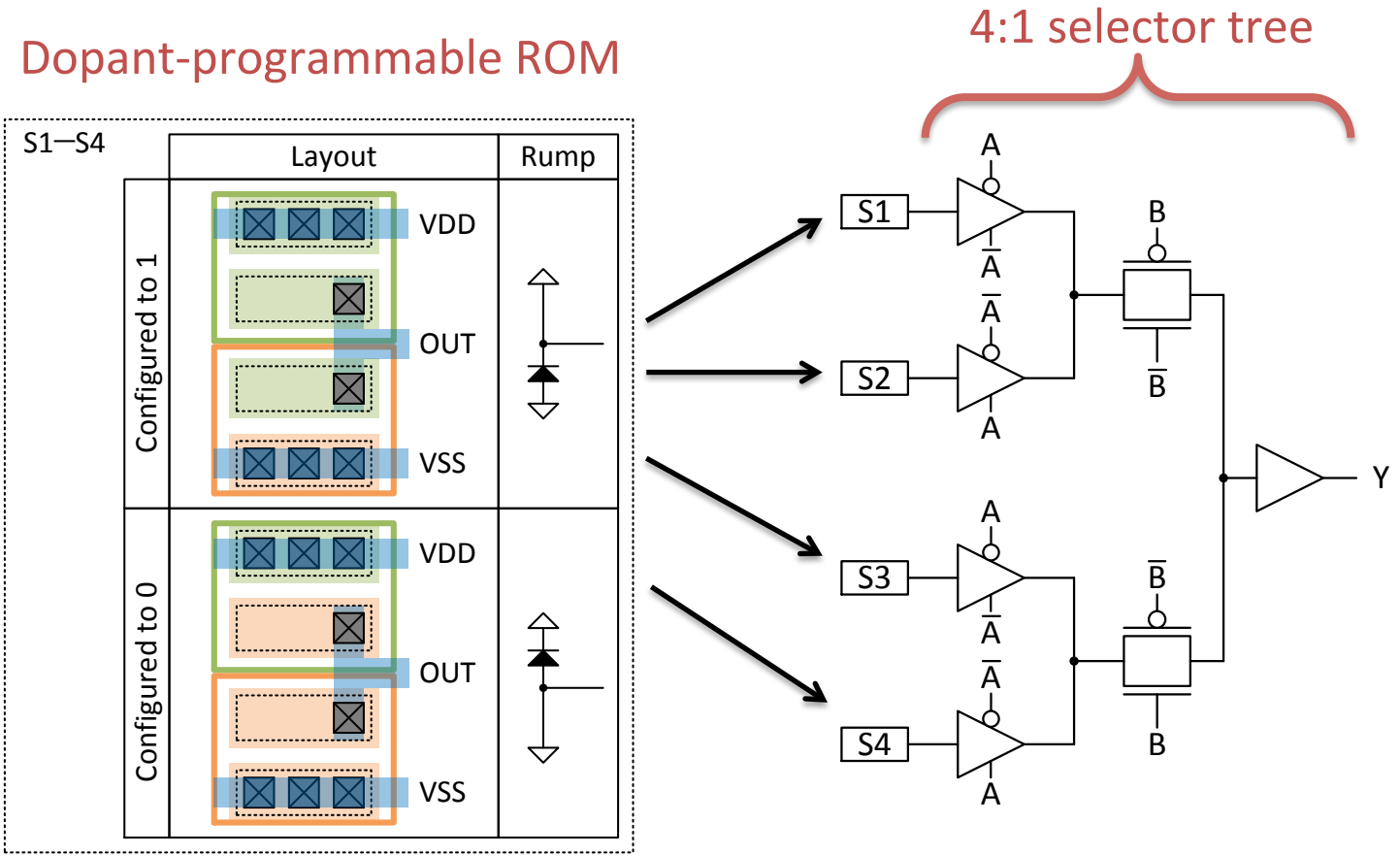
Dopant-level trojan by Becker et al. (CHES2013)

- A permanent fault is made by modifying dopants
  - A malicious fab may make such a modification at mask level
  - Various trojans can be made using the technique



DPD: Dopant-Programmable Device by Shiozaki et al.

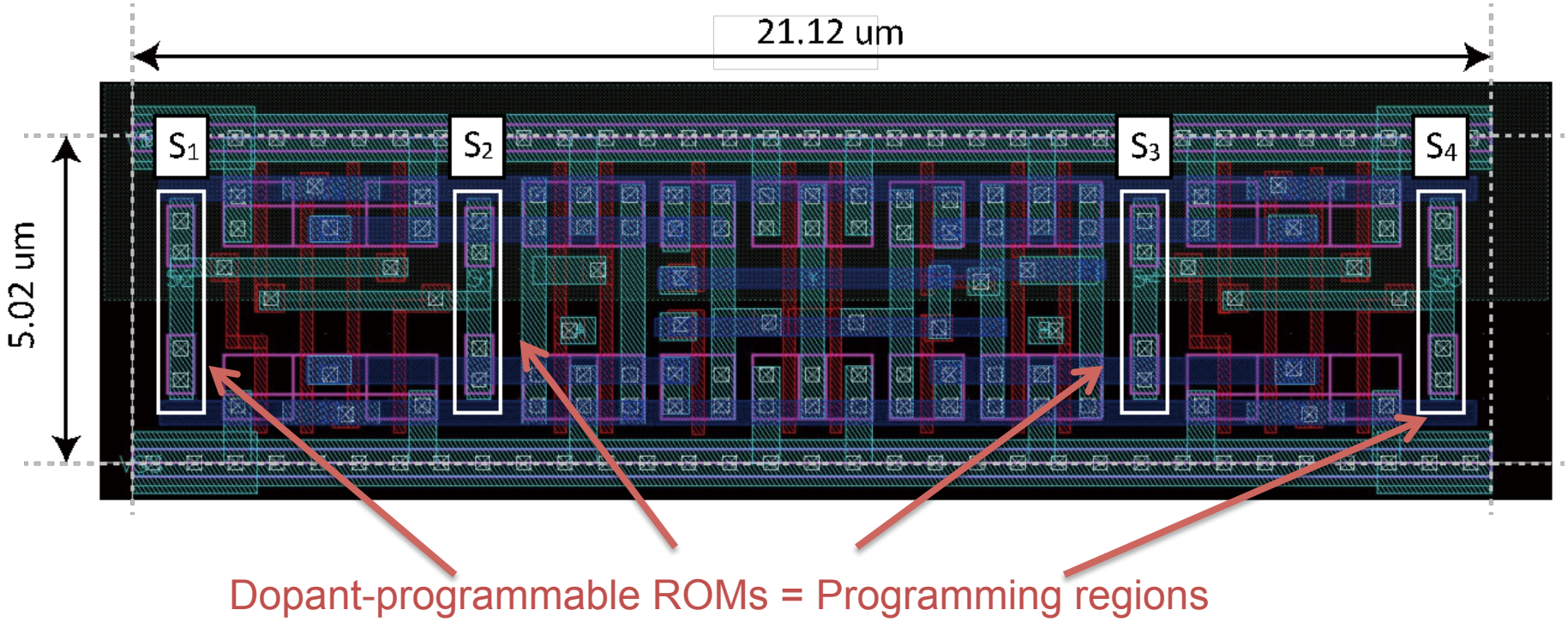
- Anti reverse engineering technique based on the same principle
  - Dopant-programmable ROM is made using the permanent faults
  - A 2-bit look-up table is made using the dopant-programmable ROM
  - Finding the LUT's functionality is as difficult as finding the trojan



Layout design of DPD cell

- The 2-bit LUT is made into a standard cell
- The configuration is determined when the active layer is designed
  - No reconfiguration after fabrication

Layout design of the DPD standard cell



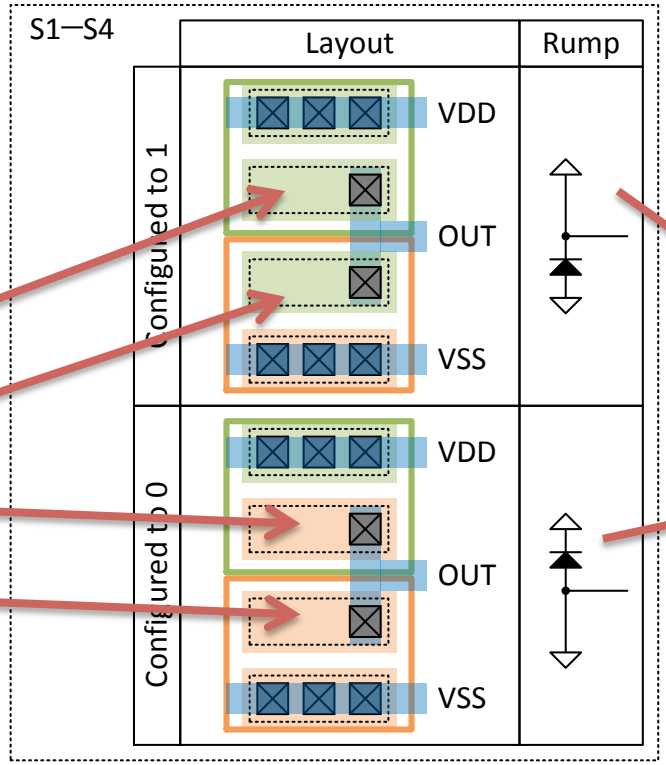
A challenge to Seeker

- Seeker wants to recover the functionality of the LUT
- Seeker needs to recover the contents of the dopant-programmable ROMs
  - There are four dopant-well combinations: {n+, p+} × {n-well, p-well}
  - Distinguishing a combination means recovering a ROM content

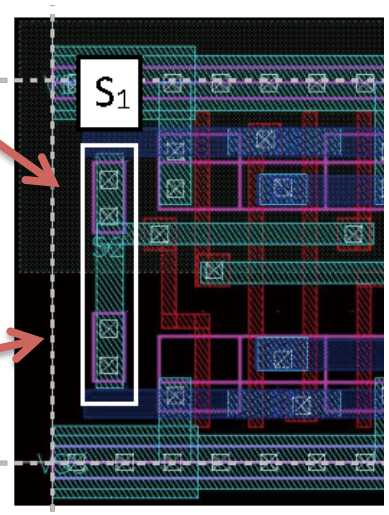
Dopant-programmable ROM

Dopant-well combinations

	Dopants	Well
ROM =1	n+	n-well
	n+	p-well
ROM =0	p+	n-well
	p+	p-well

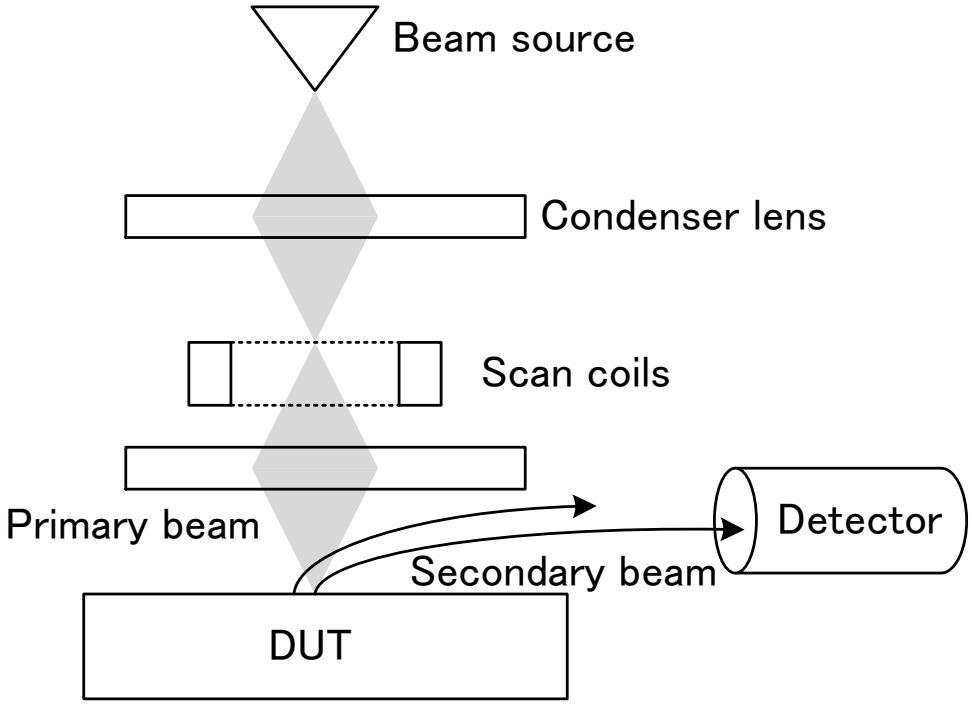


Layout



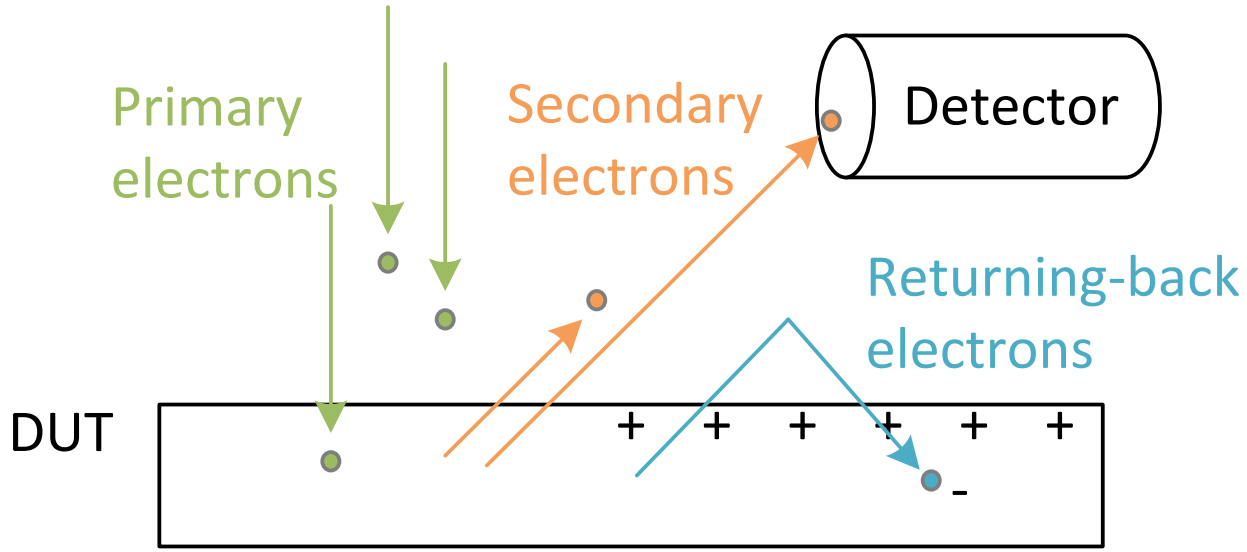
SEM: Scanning Electron Microscopy

- Measurement principle
  - Inject accelerated primary electrons to a device under test (DUT)
  - As a reaction, secondary electrons come out from DUT
    - The number of the secondary electrons is counted. That is converted to the brightness of a pixel
  - An image is made by scanning the position of the injection



PVC: Passive Voltage Contrast*

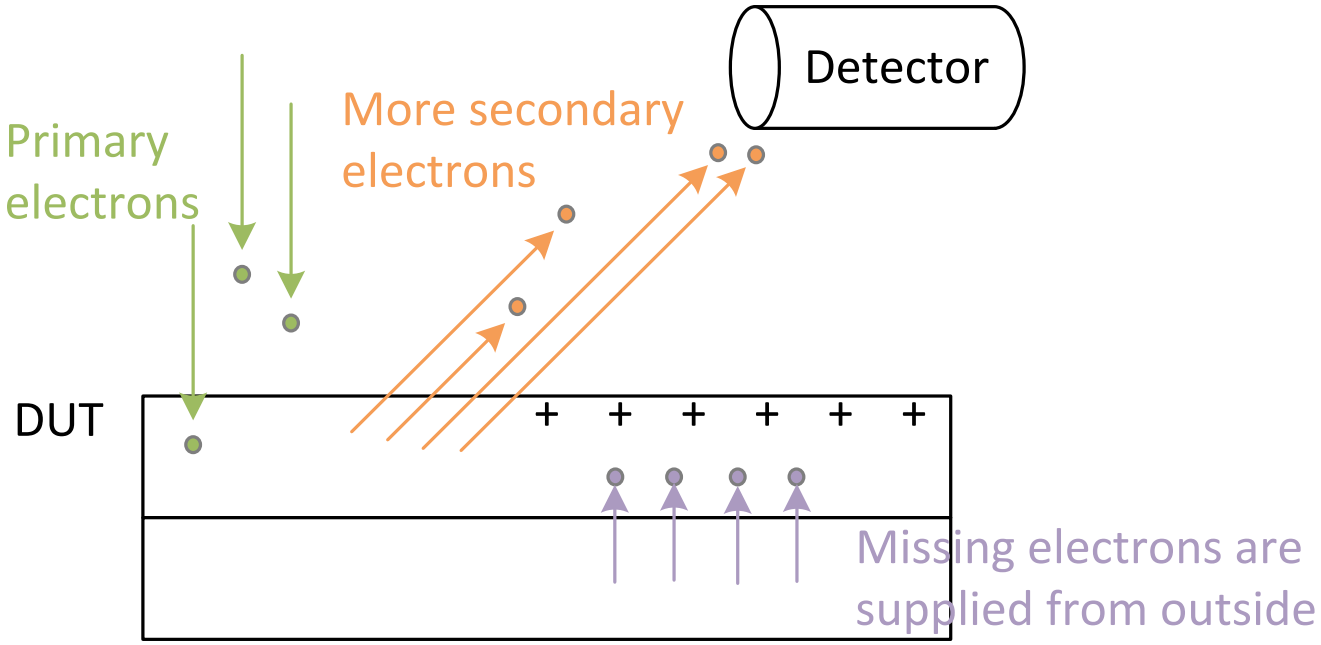
- We can measure a surface voltage of DUT with SEM
- When DUT is positively charged, some of the secondary electrons are attracted back to the sample
  - Less is measured at the detector
  - The region with higher surface voltage look darker in a SEM image



* 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.

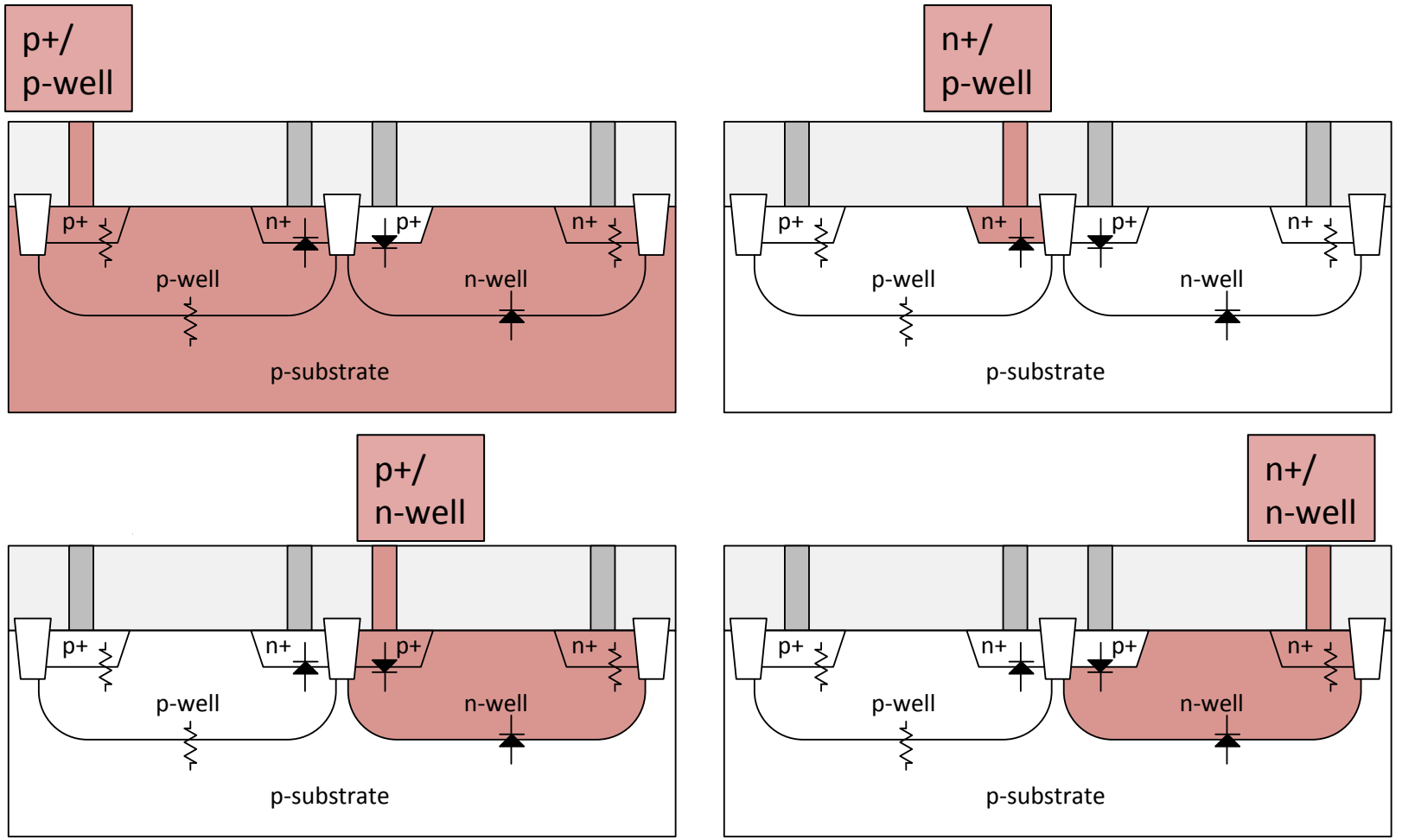
PVC: Passive Voltage Contrast cont.

- Actually, the DUT surface is charged by the primary electrons
- In a certain acceleration voltage, we observe #primary < #secondary
  - Consequently, DUT is positively charged (electron starving)
  - At the same time, electrons are supplied from outside
    - The final surface voltage is high if there is a poor supply
    - The final surface voltage is low if there is a rich supply



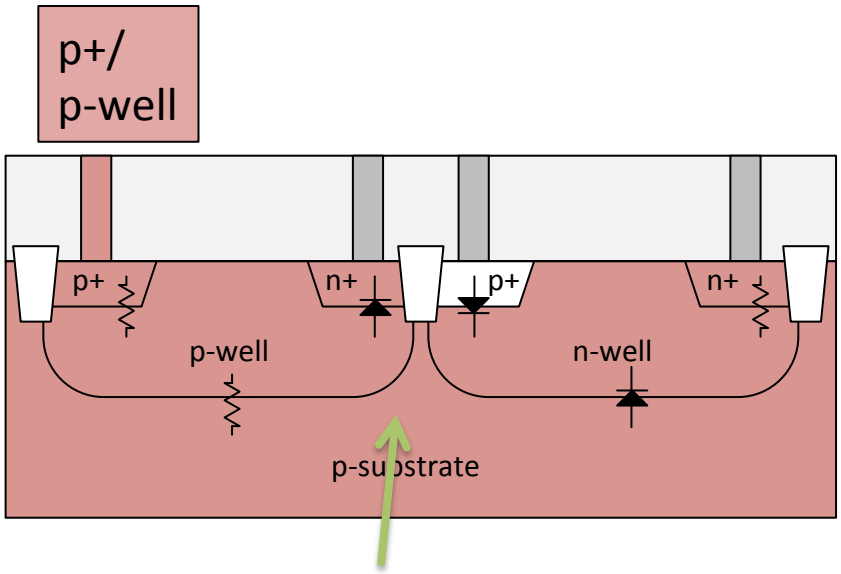
Dopant-well combinations should look differently

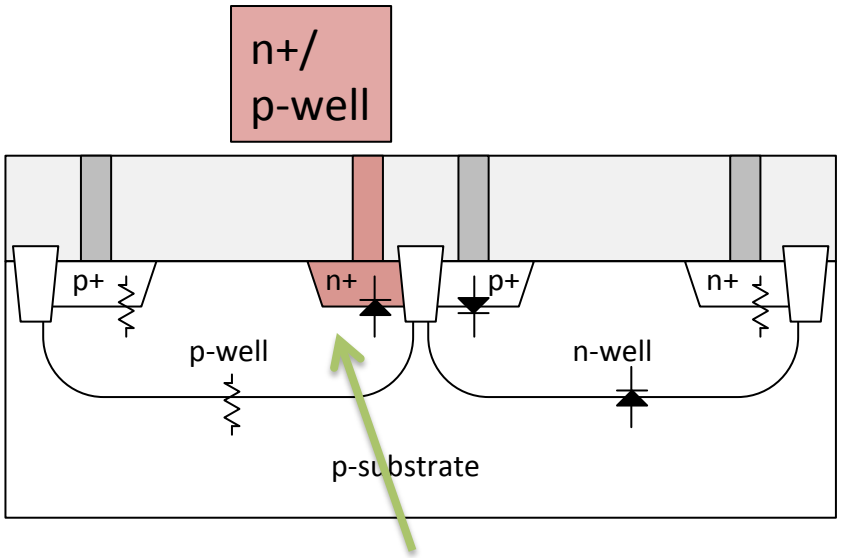
- The size of the conductive region determines the capacity to provide charges
- That is determined by the dopant-well combination
  - The diodes made by PN junctions limit the current paths



Dopant-well combinations should look differently cont.

- The size of the conductive region determines the capacity to provide charges
- That is determined by the dopant-well combination
  - The diodes made by PN junctions limit the current paths



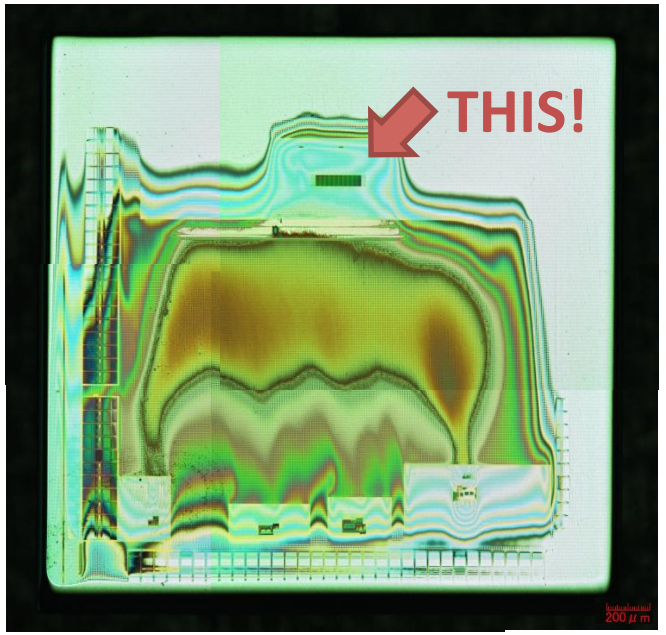


Large conductive region
= rich charge supply
= low surface voltage
= brighter pixel

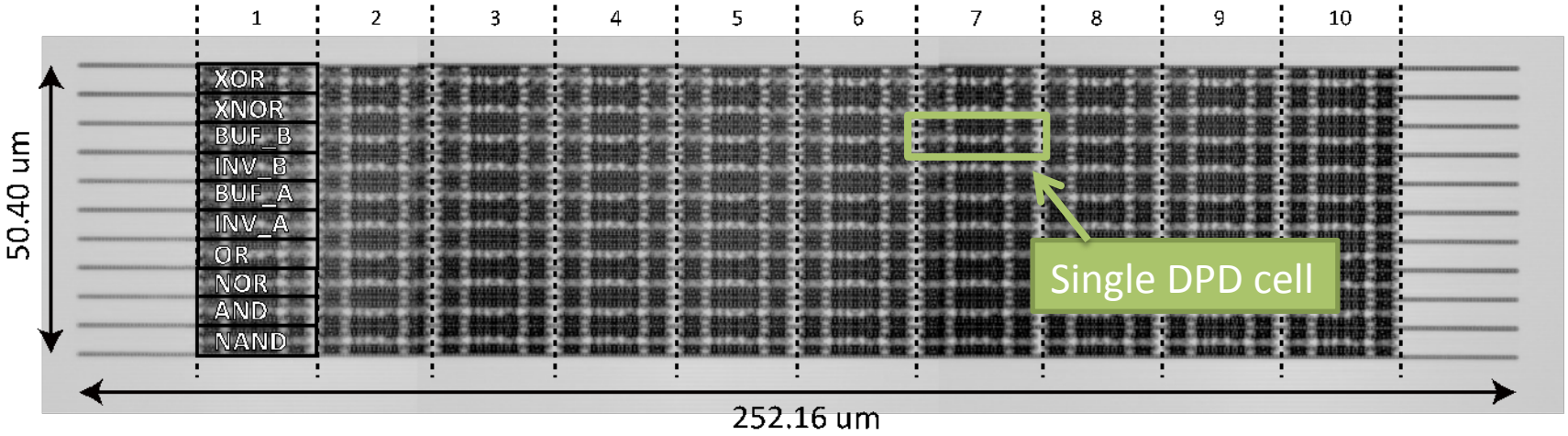
Small conductive region
= poor charge supply
= high surface voltage
= darker pixel

Measuring a target chip

- A chip containing an array of DPD cells
  - Rohm 180-nm CMOS process
  - Contact layer is exposed with mechanical polishing
  - 10 different LUT configurations × 10 each



A magnified view of the array

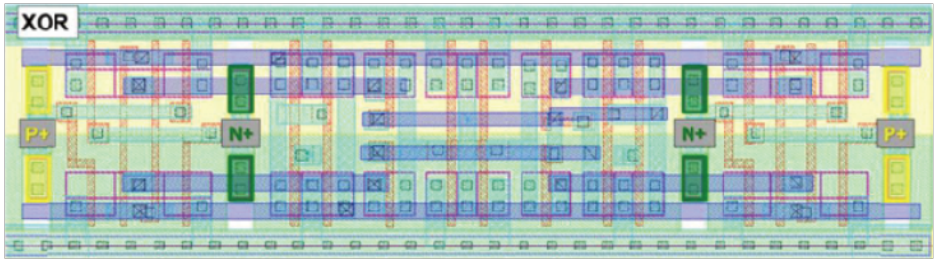


MITSUBISHI ELECTRIC
Changes for the Better

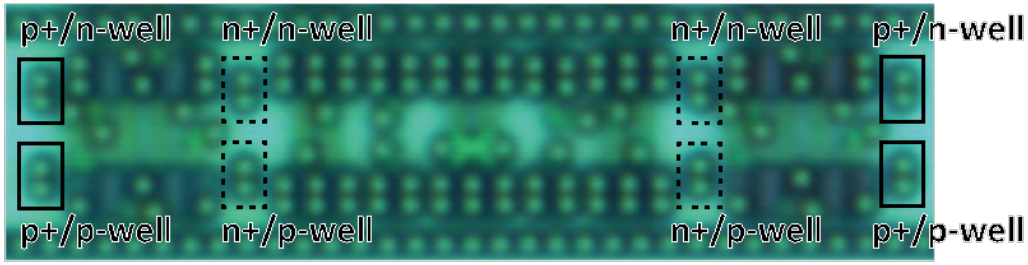
Comparing measurements

- Stealthy dopant-level circuits are measurable

(1) Layout

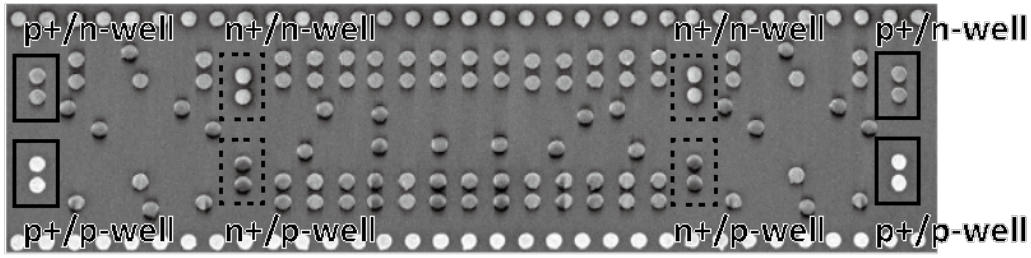


(2) Optical microscope x100

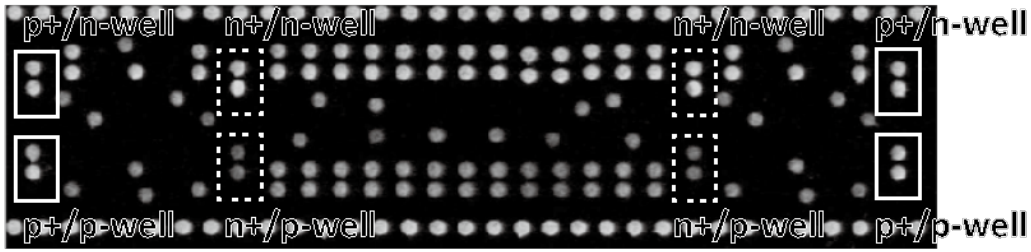


Hardly distinguishable

(3) SEM x8.0k

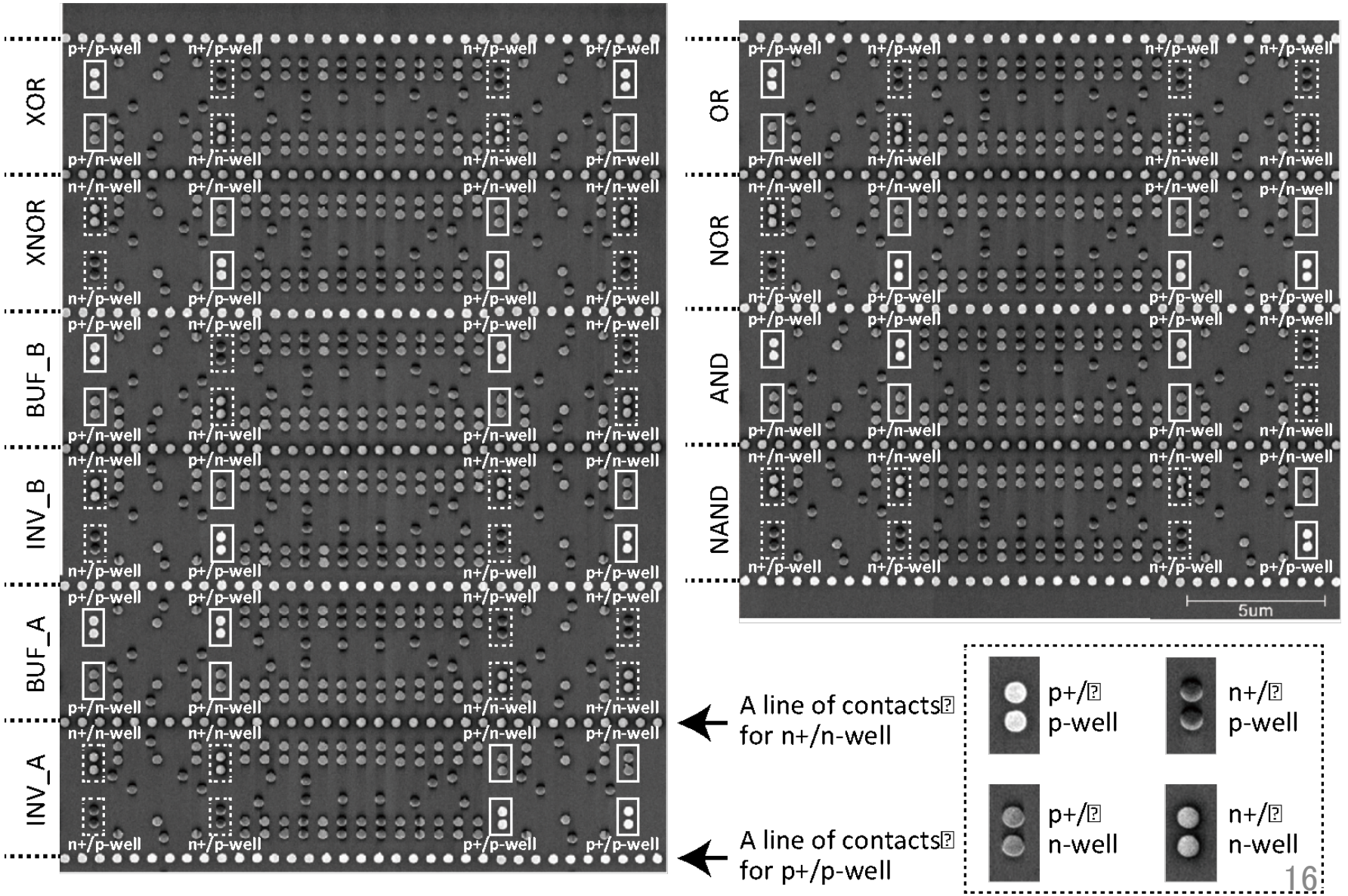


(4) FIB x12.0k



Brightness differences on the contacts

Measuring different DPD cells with SEM

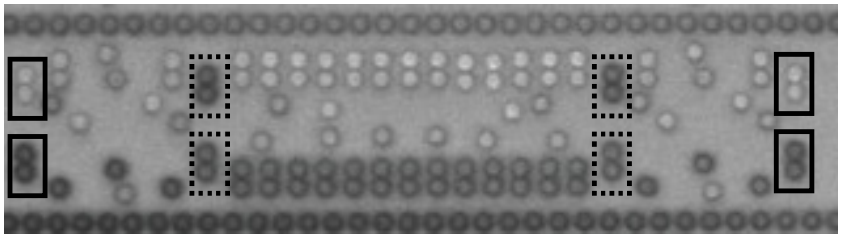


An additional cost to analyze the dopant-level circuits

- Measurement of one additional layer (the contact layer)
  - Currently, that is as expensive as the M1 layer
  - If we want to distinguish all the four cases, we need 4-times higher magnification
    - The number of images can increase up to x16

Magnification	p+/p-well	p+/n-well	n+/p-well	n+/n-well
x100, x400	---	---	---	---
x1.5k	Black	White	Black	Black
x6.0k -- x30.0k	White	Dark grey	Black	Light grey

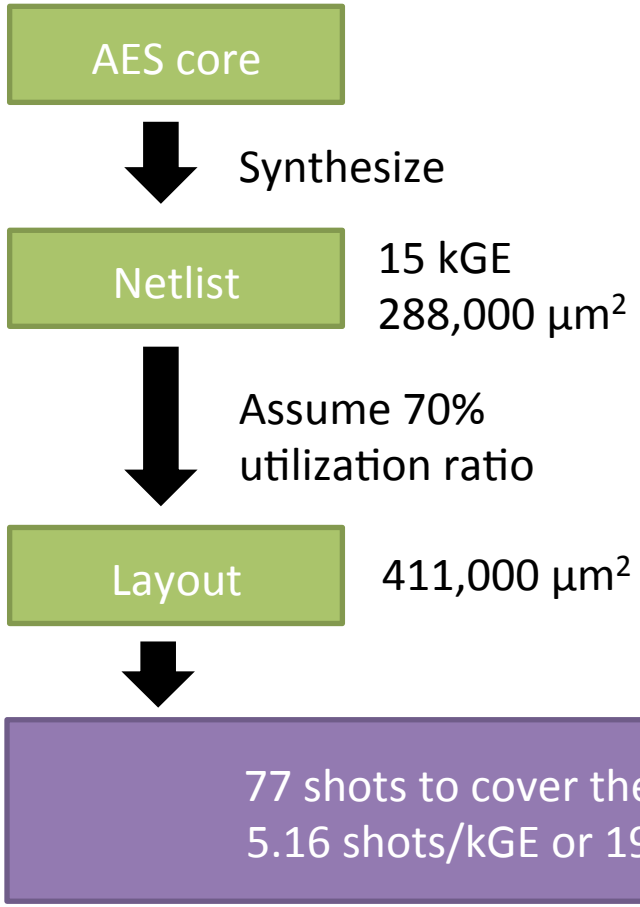
SEM, 0.7kV, Slow, x400



SEM, 0.7kV, Slow, x1.5k

An extra: how many gates in a single photo?

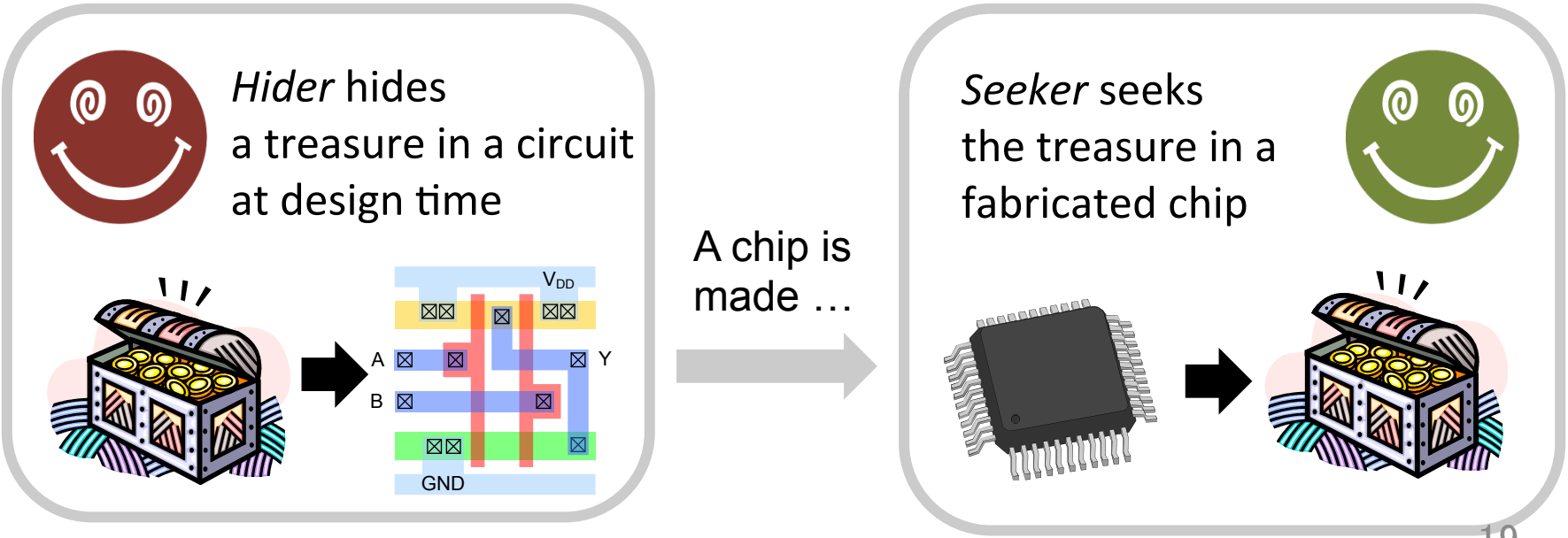
- Relationship between the gate counts and the number of images is estimated



- AES_Comp.v from Tohoku Univ.
  - 1-round/cycle design with 16 Sboxes
- The standard cell library for Rohm 180-nm CMOS technology developed by Kyoto Univ. and Kyoto Inst. Technology
- The result will scale for advanced technologies

Conclusion & open problem

- The conventional assumption of the stealthy dopant-level circuits is too optimistic
  - A good news for detecting trojans, a bad news for anti reverse engineering
- An open question: can we satisfy the conflicting goals?
  - We want *Hider* to win in anti reverse engineering
  - We want *Seeker* to win in trojan detection



Thank you!