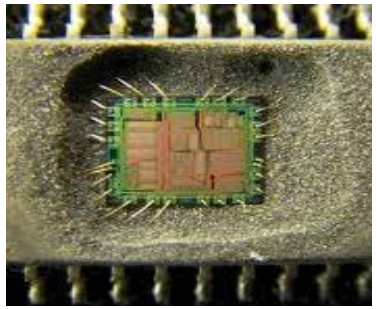
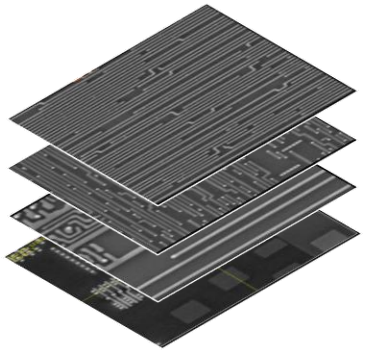
Covert Gates: Protecting Integrated Circuits with Undetectable Camouflaging

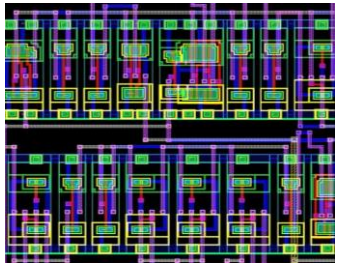
Bicky Shakya, Haoting Shen, Mark Tehranipoor and Domenic Forte

Rise of Automated Reverse Engineering

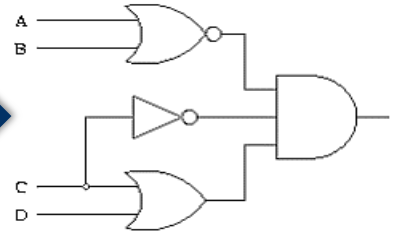




Source: Quijada, Raul, et al., *Journal of Hardware and Systems Security, (2018)*



Source: scienceasart.org



Chip

De-packaging

Chemicals & Abrasion

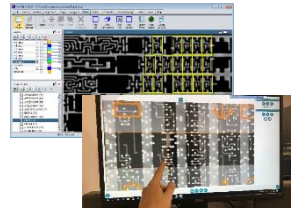
De-layering & Imaging

Polishing & Delayering

Layout Generation

Auto + Manual Analysis

Netlist Extraction



Source: micronetsol.net, texplained.com

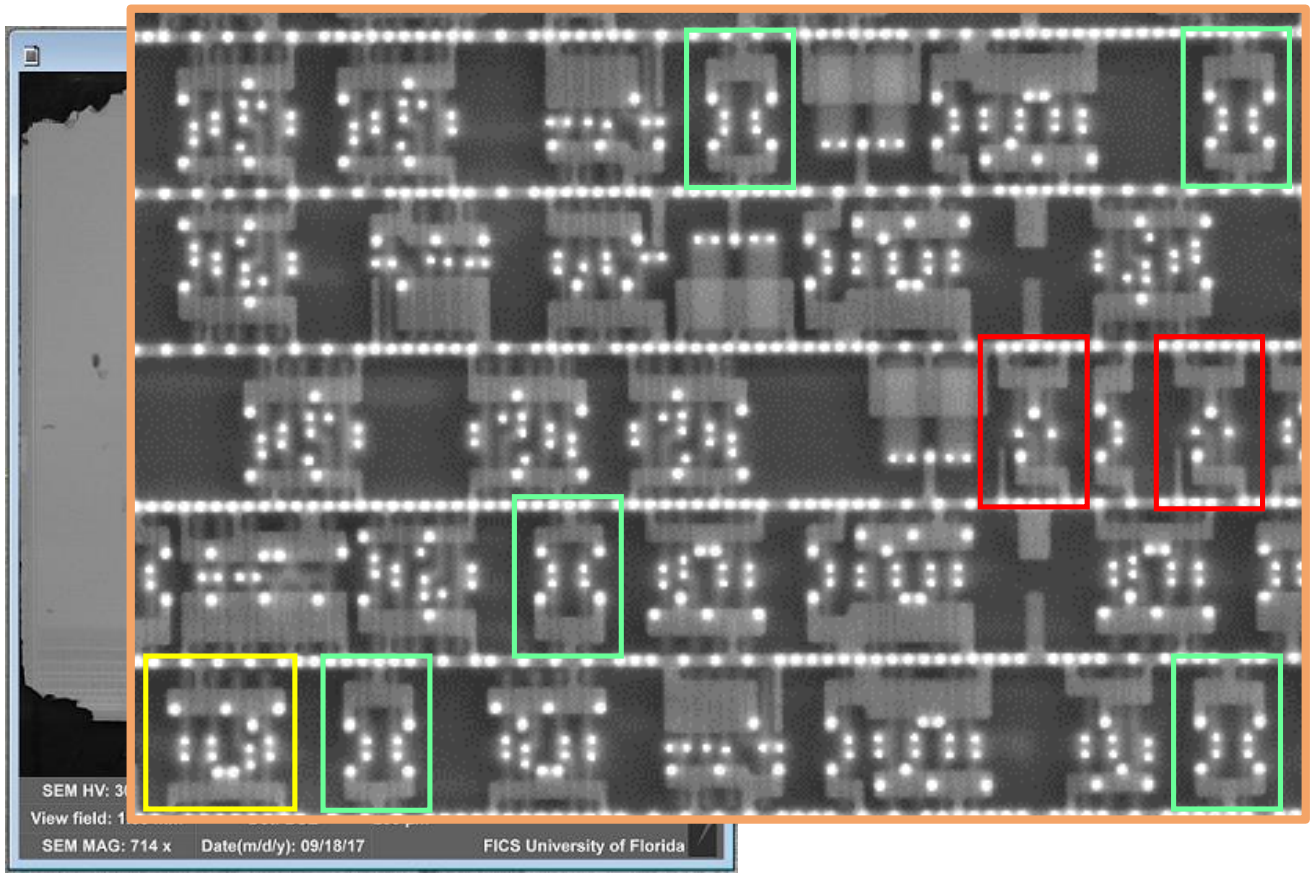
- ❑ Evaluate its performance and functionality
- ❑ See if it infringes your patents
- ❑ See how competitor product matches up

- ❑ Integrate the IP into an attacker's design
- ❑ Clone the design
- ❑ Find and exploit vulnerabilities in the design

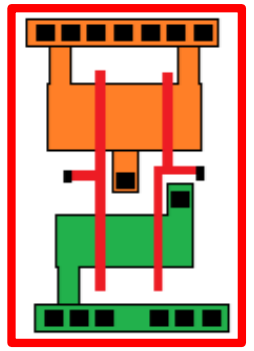
What is IC Camouflaging?

Main Goal: Protect IP from Reverse Engineering

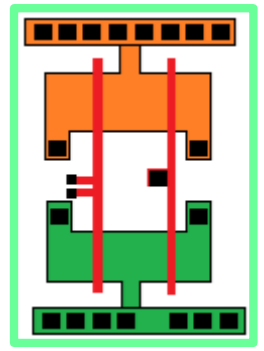
Stakeholders: Commercial Semiconductor Design Houses and Fabless Vendors, IP Providers (even Foundries), and Government (esp. Defense)



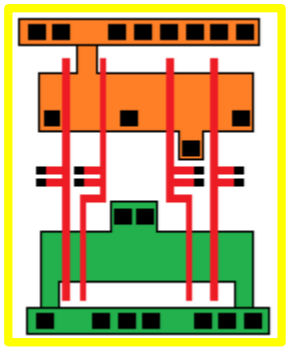
NAND

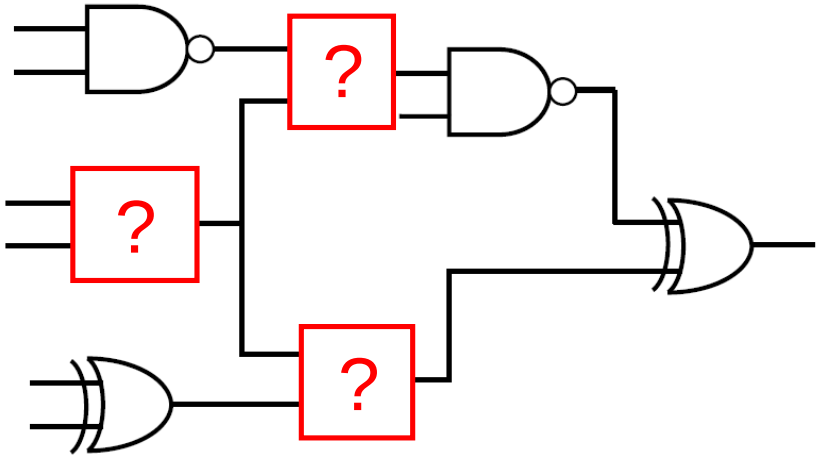


Buffer



AOI22

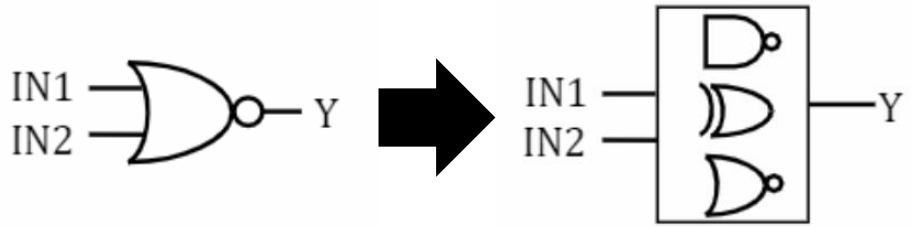




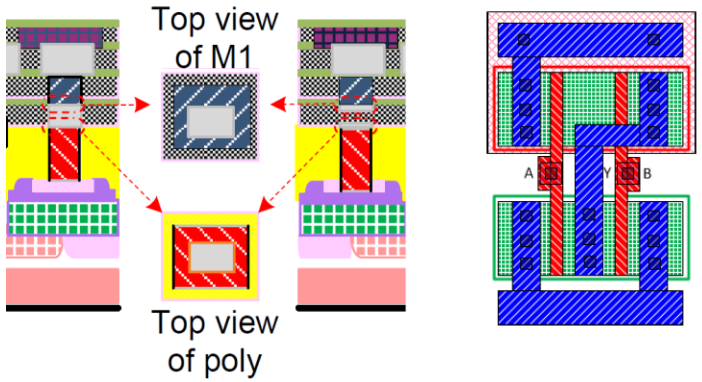
***Camouflaged* Netlist**

Existing Camouflaging Techniques

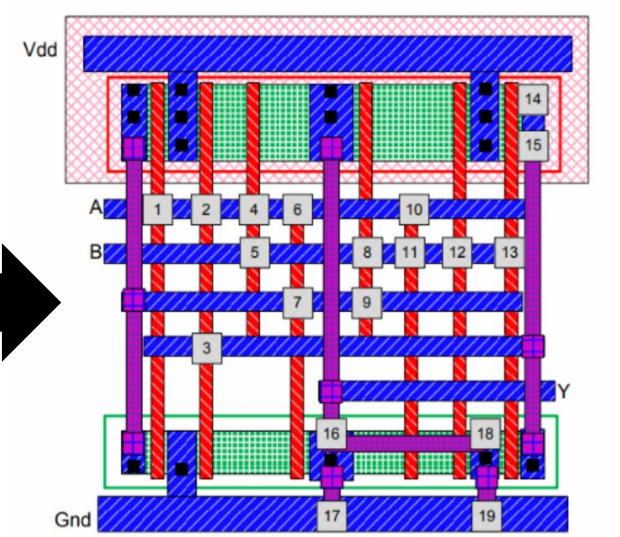
Camouflaging (Camo) Gate: hide the real gate's function



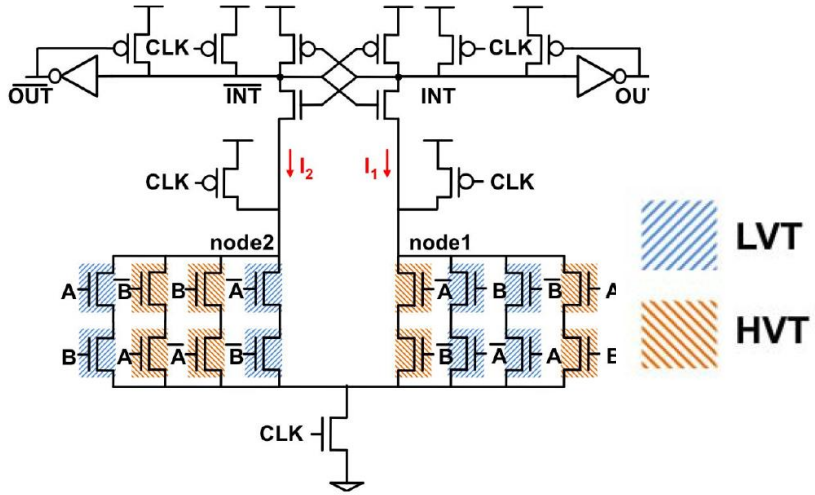
Camouflaging Gate Design Examples



Dummy Contact
[Rajendran et al, CCS 2013]



Threshold-Voltage Modification
[Erbagci et al., HOST 2016]



Drawbacks

- 4-5x Larger Power and Area
- Different Logic Style
- > 2x Area, 1.5x Delay, and 10% Power

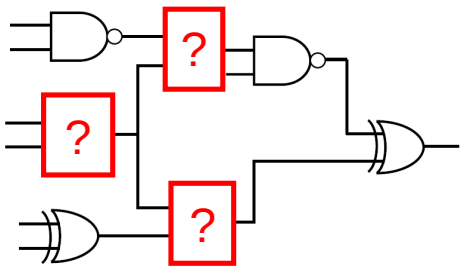
Scope and Adversarial Model

Assumption #1 (Defense): Foundry is trusted

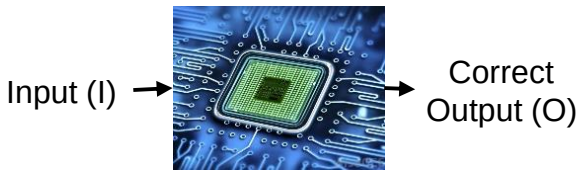
- Plays an active role in protecting the IP
- May even provide library of camo cell technologies
- Does not leak GDSII, mask sets, etc.

Assumption #2 (Attack): The following are available to the attacker

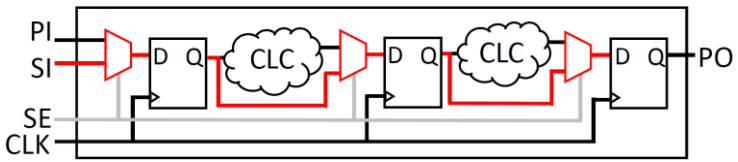
- ❑ A *Camouflaged* Netlist (obtained by RE)



- ❑ A Functional Chip (i.e., Oracle)



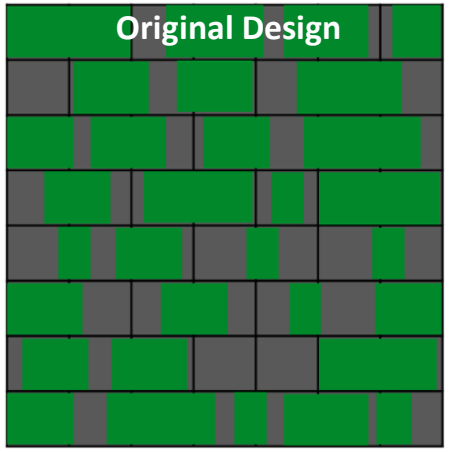
- ❑ Scan Chain Access

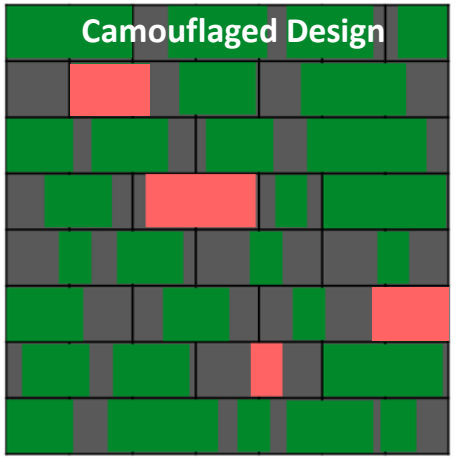


Attacks on Prior IC Camouflaging Approaches

Cell identified by RE

Cell not identified by RE

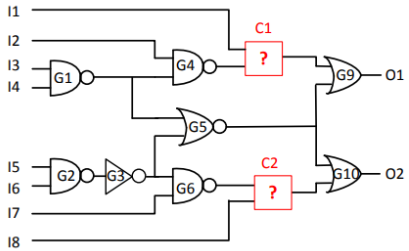




Overhead Cost → Limited No. of Camouflaging → Attack Vector

Automatic Test Pattern Generation (ATPG)

[Rajendran et al., DAC 2012, Vontela et al., ISQED 2017]

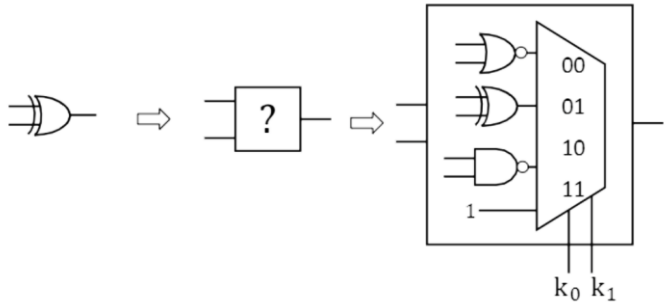


Steps:

1. Build equivalent circuit encoding (camo → logic locked)
2. Apply input patterns at PI, scan-in to sensitize camo gate inputs
3. Use test response to resolve gate functionality

Satisfiability-based (SAT) Attack

[Massad et al., NDSS 2015, Subramanyan et al., HOST 2015]



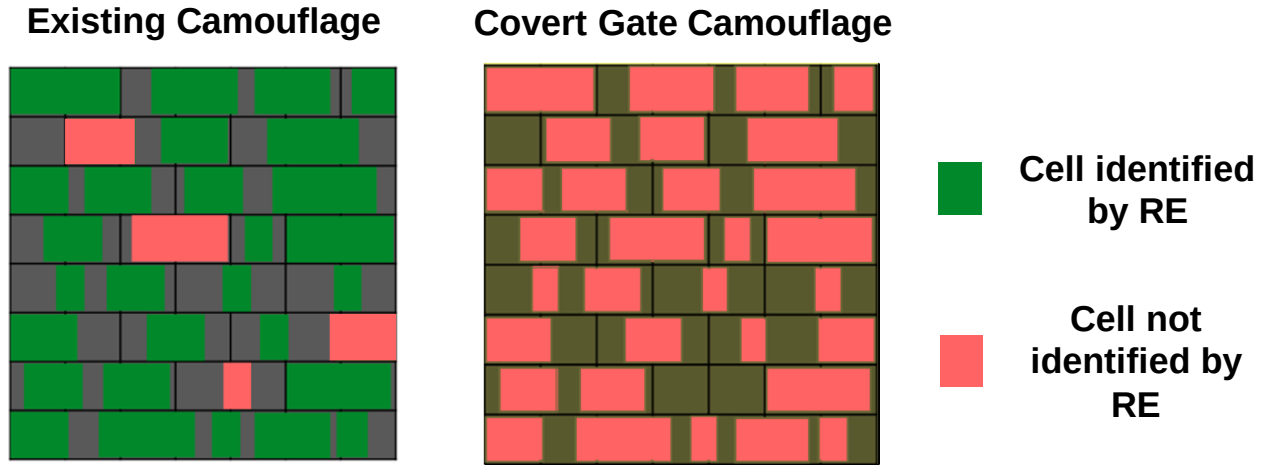
Steps:

1. Build equivalent circuit encoding
2. Observe the satisfiability using oracle
3. Rule out incorrect assignments

Proposed Approach: ‘Covert’ Camo Gate

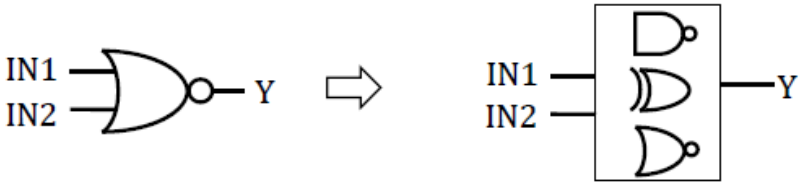
Requirements

- Every camouflaged gate should look like any other gate in a standard cell library
  - All gates become suspect!
  - Expected to drastically increase invasive and non-invasive attack complexity

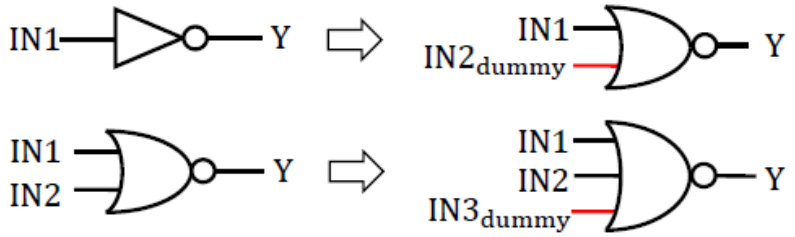


Covert Gate

- Expand n input gates into $n + i$ input gates (where i is # of dummy inputs)
  - \+ Much lower leakage/area/delay expected with dummy inputs
  - \+ No change in logic style



Existing Camouflage



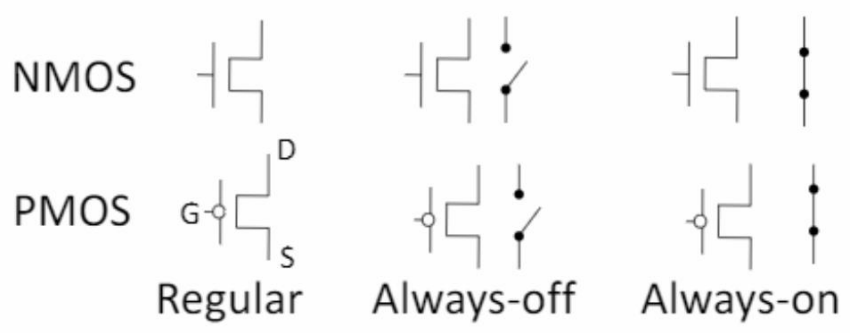
Covert Gate Camouflage

‘Covert’ Gate Schematic Design

Regular MOSFET modification

Switchable transistors → [Always-On] or [Always-Off]

Modification is <u>INVISIBLE</u> by SEM



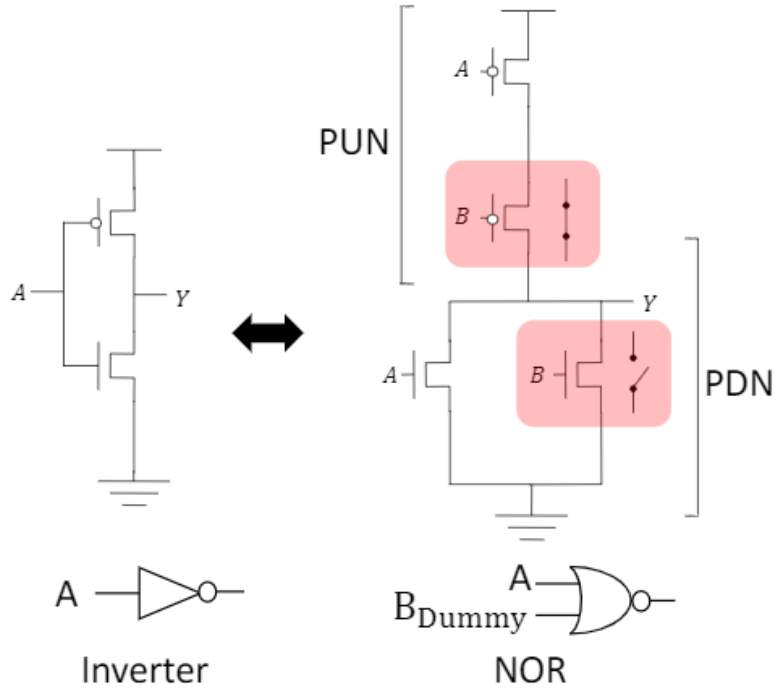
Complementary structure is necessary:

1. Enable functional gates
2. Keep the static current leakage low

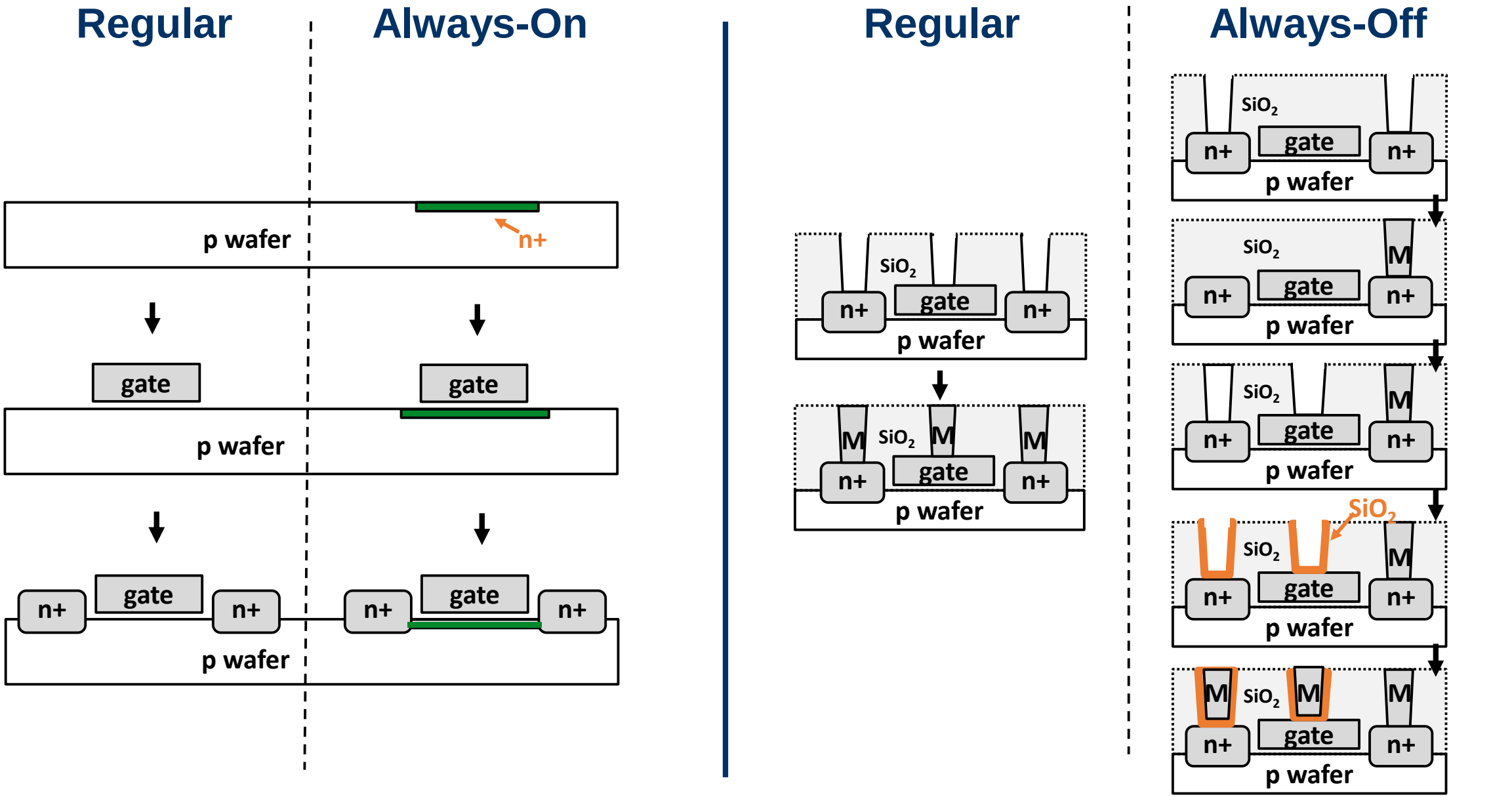
Implemented modification: <u>Dummy Inputs</u>

- Always-On in the pull-up
- Always-Off in the pull-down

- Always-Off in the pull-up
- Always-On in the pull-down

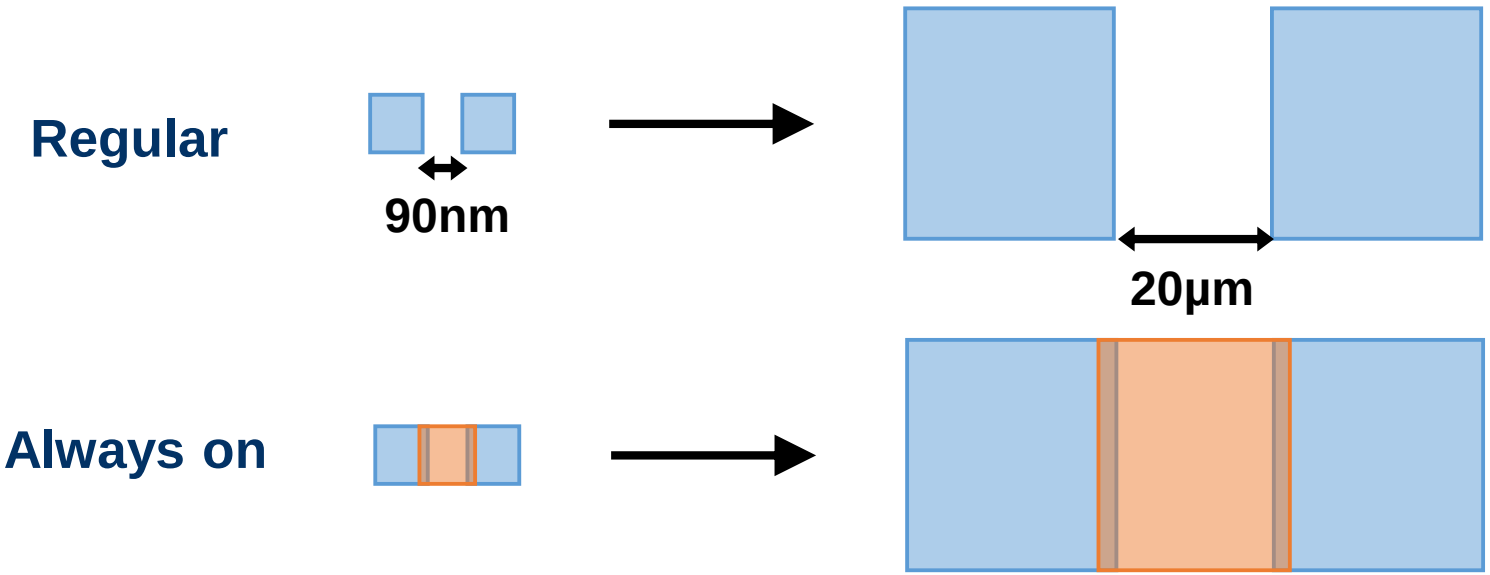


Device Structure and Fabrication of Covert Gates



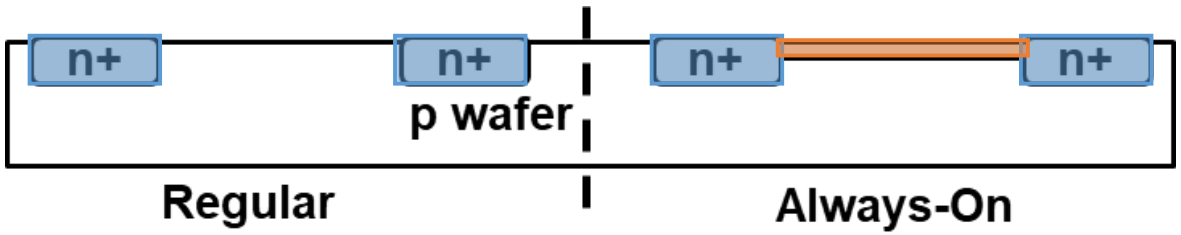
‘Always on’ Prototype Structure

Top-views



Regular doping (source/drain) Shallow doping (always-on channel)

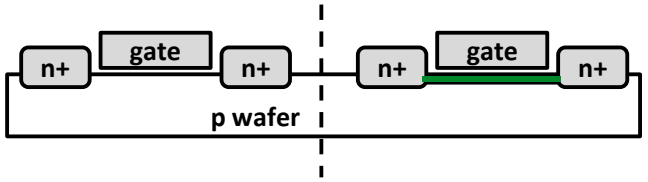
Cross-sections



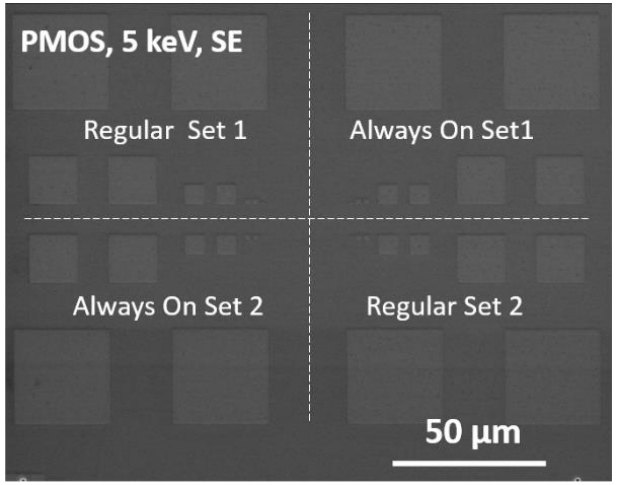
TESCAN LYRA-3

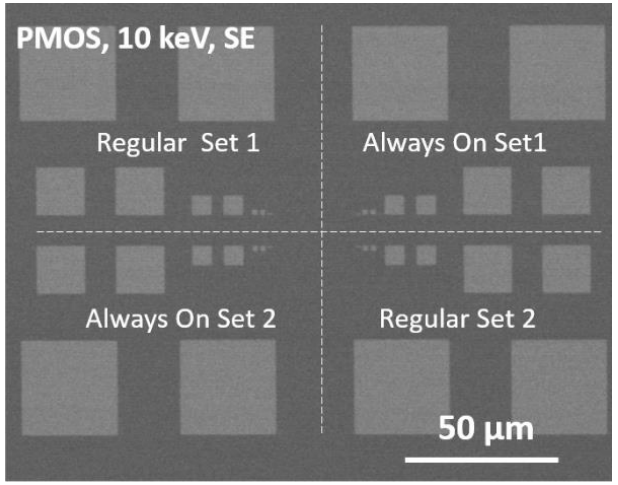
Imaging Settings	
SE	**BSE**
15 keV	15 keV
10 keV	10 keV
5 keV	5 keV
800 eV	N/A

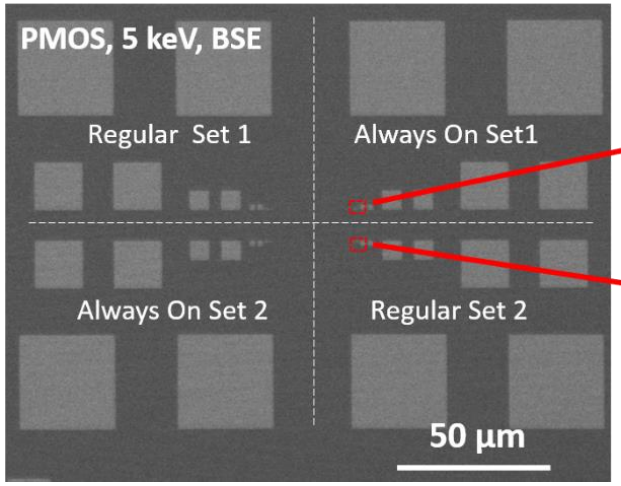
Imaging Results – Regular vs. Always-On

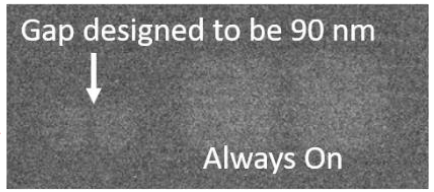


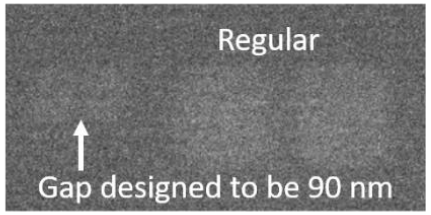
PMOS



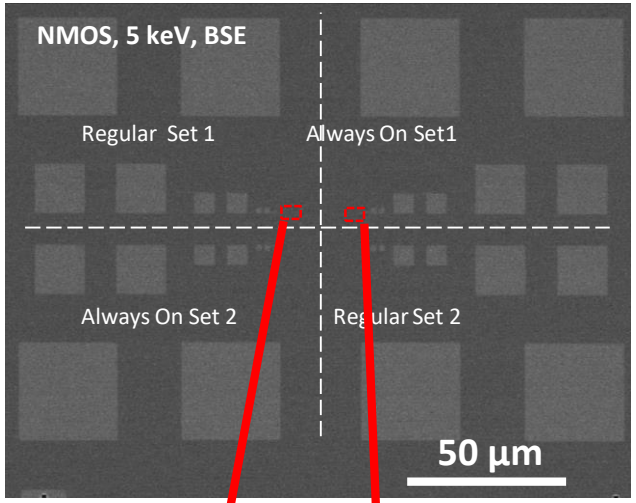


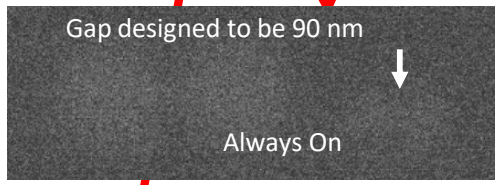


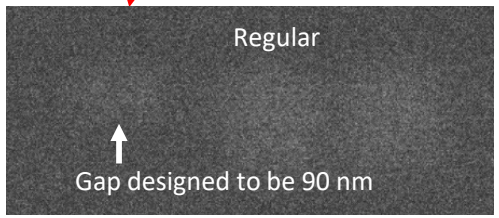




NMOS

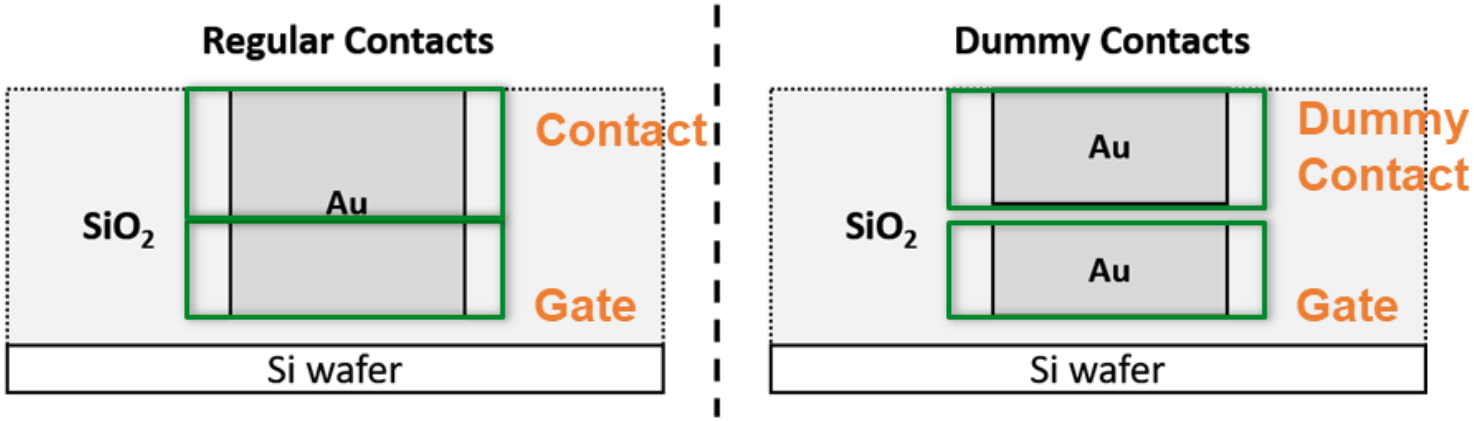




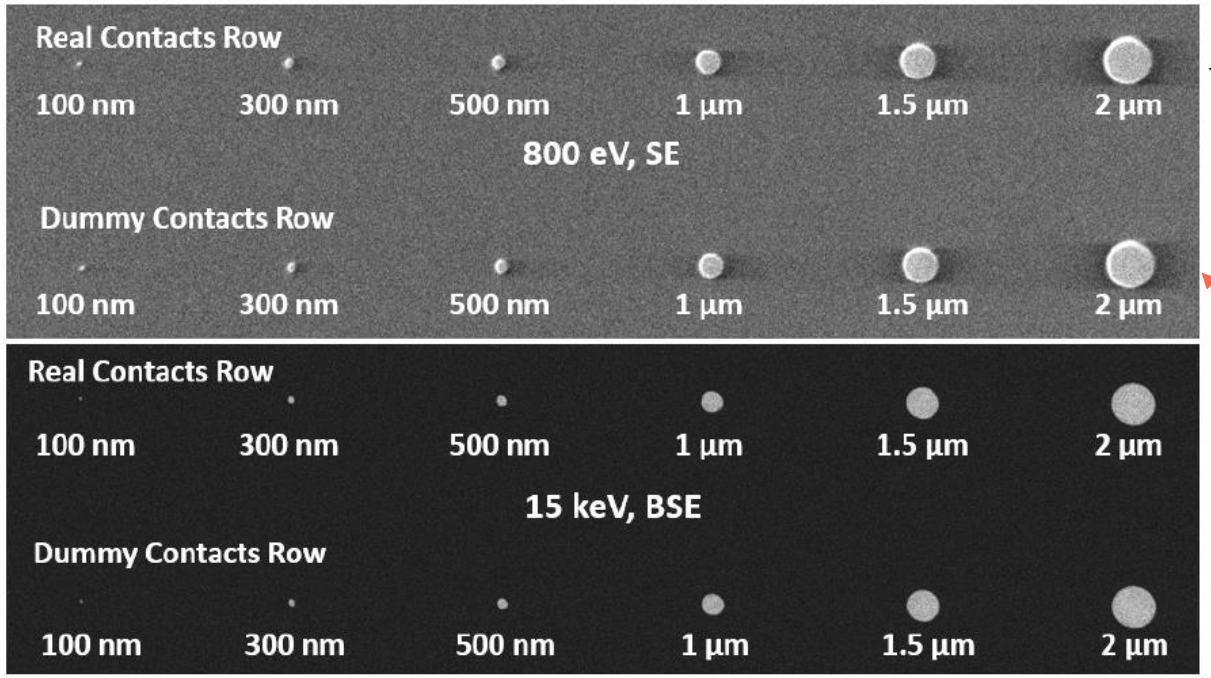


Imaging Results – Regular vs. Always-Off

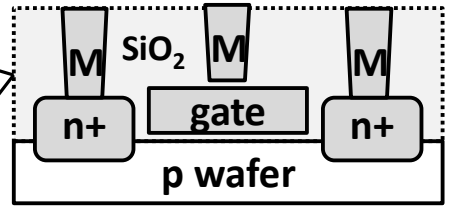
Cross-section (Prototype)



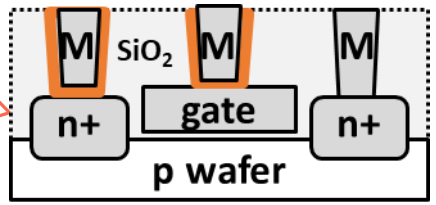
Top View (SEM) Top: SE Bottom: BSE



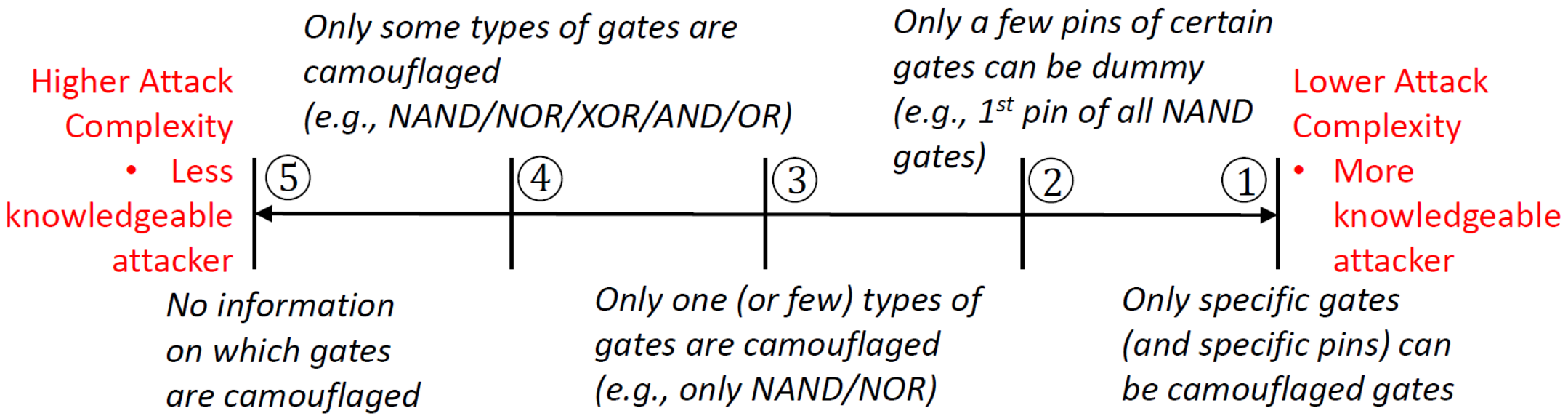
Regular



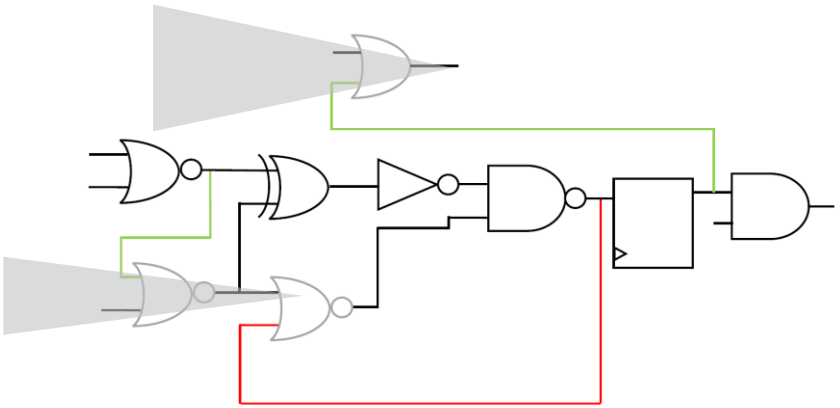
Dummy



Experimental Setup

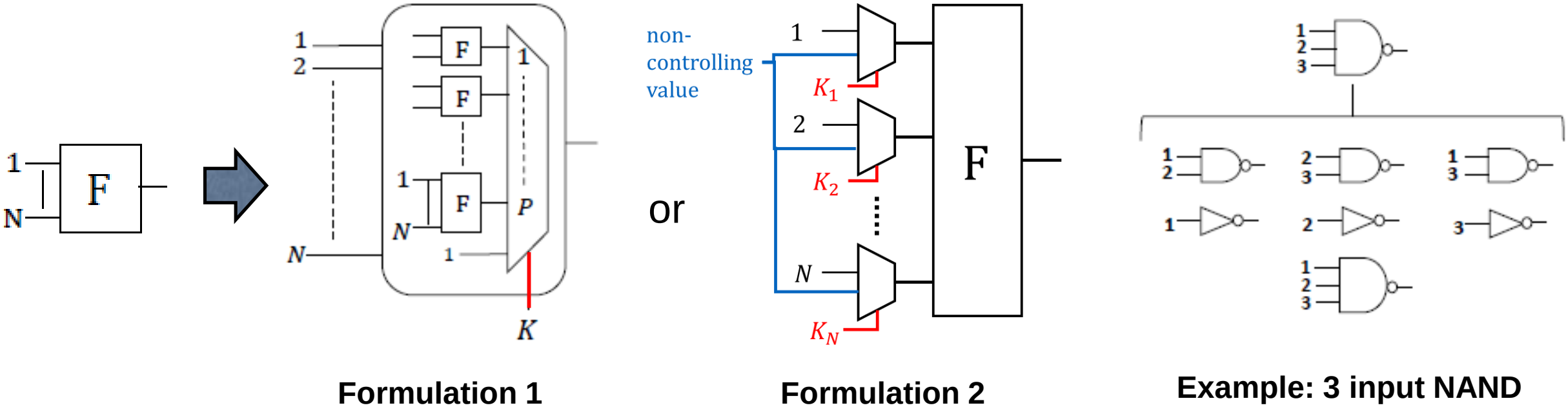


- **SAT Attack:** Scenario #3, timeout set at 12 hours
- **Test-based Attack:** Scenario #2
- **Covert Gate Insertion:** Random, but combination feedbacks are not allowed



Fan-in cone modification, enabled by dummy inputs

SAT Attack Formulation on Covert Gates



- Correct key chooses correct pins **based on oracle response**
- **Complexity increase** with
  - No. of pins on suspect gates
  - No. of candidate gates → *all gates*
  - Increased conjunctive normal form (CNF) formula size → *Larger search space*

SAT Attack Results

Benchmark	Gate / Node Count	Existing Camo		Proposed Camo (Covert)	
		$\|K\|$	Attack Time (s)	$\|K\|$	Attack Time (hrs) Form 1 [Form 2]
C1908	880	34	0.55	811	3.52 [5.91]
C2670	1193	26	0.65	1514	Timeout [Timeout]
C3540	1669	28	0.68	2088	Timeout [Timeout]
C5315	2307	46	3.58	3379	Timeout [4.27]
C7552	3512	106	4.07	4454	Timeout [Timeout]
arbiter	11,839	1182	3815.00	23,678	Timeout [Timeout]
voter	13,758	1078	Timeout	21,560	Timeout [Timeout]

SAT Attack Complexity

- ❑ Increased key size
- ❑ SAT attack timeout (12 hrs)→ More iterations / More time per iteration

Test-Based Attack Results

Generate a test to check whether pin is dummy or functional.

- **Control:** Assert controlling value on suspect pin (using s-a-0, s-a-1)
- **Observe:** Non-controlling values on other pins and nets to propagate to observe point

Legend

Attack succeeds

Attack fails

Possible Scenarios

- **Detectable:** it can be determined with certainty whether a pin on the gate is dummy or not
- **Undetectable:** the dummy pin has no effect on the output 'ATPG
- **Untestable:** a test pattern cannot be generated to sensitize and propagate a controlling value on a potentially dummy pin
- **Not Detected:** test pattern to detect the pin could not be generated with tool effort level

> 91%

Benchmark	Gate	Gate Count	Detectable		Undetectable		ATPG Untestable		Not Detected	
			#	%	#	%	#	%	#	%
b18 Primitive Count = 84,632 #Scan DFF = 3,020 I/O = 40/24	NOR2X	2390	10	0.42	5	0.21	2873	99.29	2	0.08
	NOR3X	270	12	4.44	0	0.00	237	87.78	21	7.78
	NOR4X	195	17	8.72	0	0.00	114	58.46	64	32.82
	NAND2X	4194	7	0.17	30	0.72	4154	99.05	3	0.07
	NAND3X	2135	8	0.37	19	0.89	1849	86.60	259	12.13
	NAND4X	909	38	4.18	0	0.00	753	82.84	118	12.98

Circuit Overhead and Corruptibility Results

Benchmark	Area (μm^2)			Delay (ns)			Power (μW)			Verification Failure (%)
	Covert	Original	%	Covert	Original	%	Covert	Original	%	
AES	114,098	113,384	0.63	18.19	15.99	13.76	2,689	2,678	0.38	80.42
b12	9,725	9,646	0.81	2.98	2.88	3.46	154	154	0.35	54.33
b15	53,432	53,134	0.56	26.32	26.32	0.00	654	657	-0.38	94.66
b17	171,193	170,264	0.54	32.47	31.14	4.27	2,015	2,011	0.22	91.37
s35932	111,402	111,088	0.28	14.13	10.84	30.35	2,290	2,328	-1.67	90.87
s38417	107,803	107,349	0.42	20.84	16.69	24.87	1.949	1,949	-0.03	54.85
s38584	87,647	87,229	0.48	15.38	13.11	17.32	1,572	1,570	0.08	70.29

- *Minimal area overhead.* Proposed camo cells are no larger than standard logic gates (AND2X1, NAND2X1 etc.)
- *Power overhead minimal*
- *Delay penalty due to random insertion.* Can avoid critical paths for further optimization
- *High Corruptability.* Even when covert gates are inserted randomly, there are large number of percentage mismatches with original design

Acknowledgements

We are grateful for the sponsors of this project:

Thank you to the partners and sponsors of UF/FICS SCAN Lab:

Conclusion and Future Work

Covert gates

- Indistinguishable from regular gates (i.e., imaging resistant)
- Very strong deterrents against oracle-based and probing-based reverse engineering
- Inexpensive to fabricate
- Lower overhead than existing camo gates

Future Work

- Formal proofs of security against oracle attacks
- Investigate oracle-less attacks (e.g., structural) against covert gate circuits
- Explore covert gate insertion strategies w/ security and overhead in mind
- Fabricate and characterize real covert gate devices
- Image using He-Ne ion microscopes

Conclusion and Future Work

Covert gates

- Indistinguishable from regular gates (i.e., imaging resistant)
- Very strong deterrents against oracle-based and probing-based reverse engineering
- Inexpensive to fabricate
- Lower overhead than existing camo gates

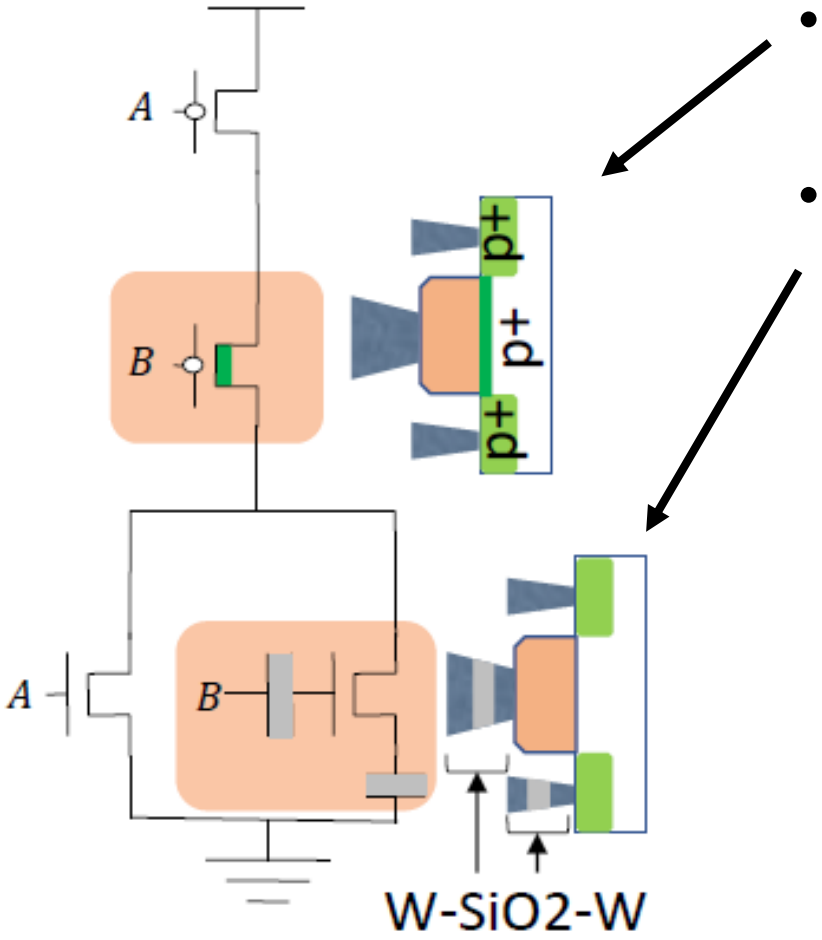
Future Work

- Formal proofs of security against oracle attacks
- Investigate oracle-less attacks (e.g., structural) against covert gate circuits
- Explore covert gate insertion strategies w/ security and overhead in mind
- Fabricate and characterize real covert gate devices
- Image using He-Ne ion microscopes

Covert Gate Distribution for SAT Evaluation

Benchmark	Total % Covert	2 input		3 input		4 input	
		AND/NAND	OR/NOR	AND/NAND	OR/NOR	AND/NAND	OR/NOR
C1908	45%	43%	0%	1%	0%	0%	0%
C2670	56%	38%	5%	9%	0%	1%	2%
C3540	56%	41%	4%	6%	5%	1%	0%
C5315	60%	34%	5%	16%	2%	1%	3%
C7552	58%	44%	6%	4%	1%	2%	1%
arbiter	100%	100%	0%	0%	0%	0%	0%
voter	100%	100%	0%	0%	0%	0%	0%

Covert Gate Circuit Model

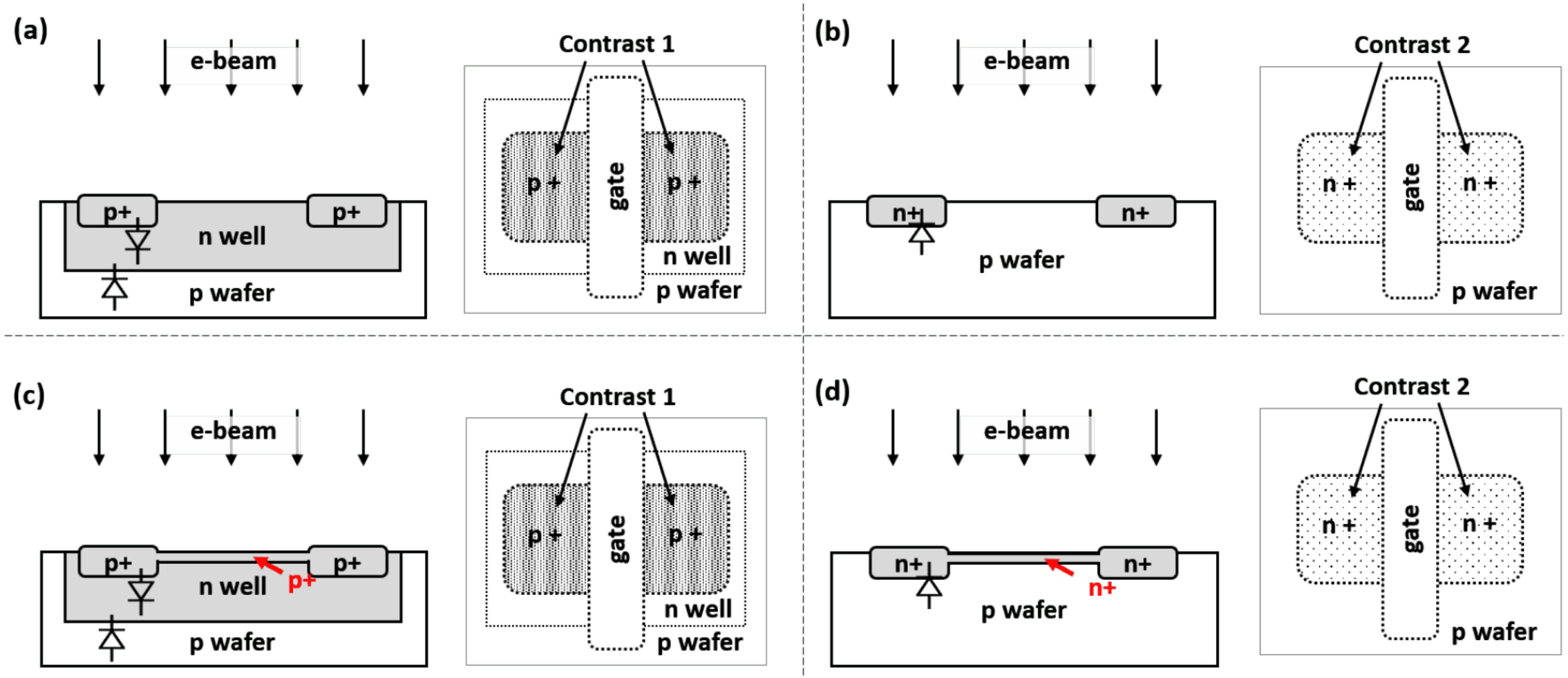


- **Always-on FET** emulated by depletion mode device where channel is ‘pre-formed’
- **Always-off FET** emulated by SiO2 insulator in gate and source contacts

Overhead Cost (SPICE Simulations)

Dummy-based Camouflaging Gates				Proposed Covert Gates (Compared to INVX1)			
Area	Delay	Power		Area	Delay	Dyn Power	Static Power
4 X	1.6 X	5.5 X	NAND2X1	0.86X	1.34 X	0.72 X	0.22X
4 X	1.1 X	5.1 X	NOR2X1	1.00X	1.82 X	0.69 X	0.27X

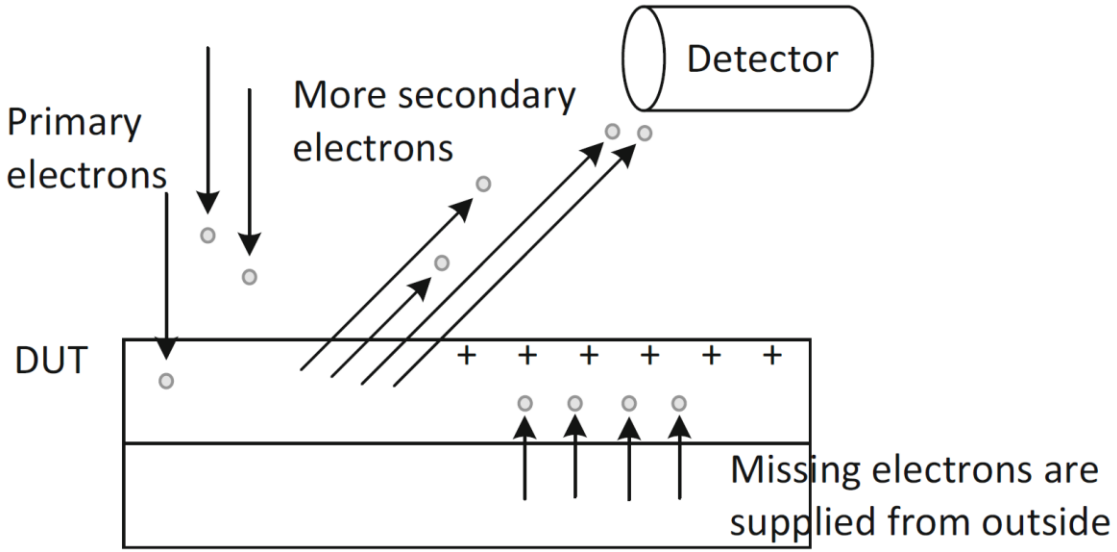
Effective Conduction Volumes (Proposed)

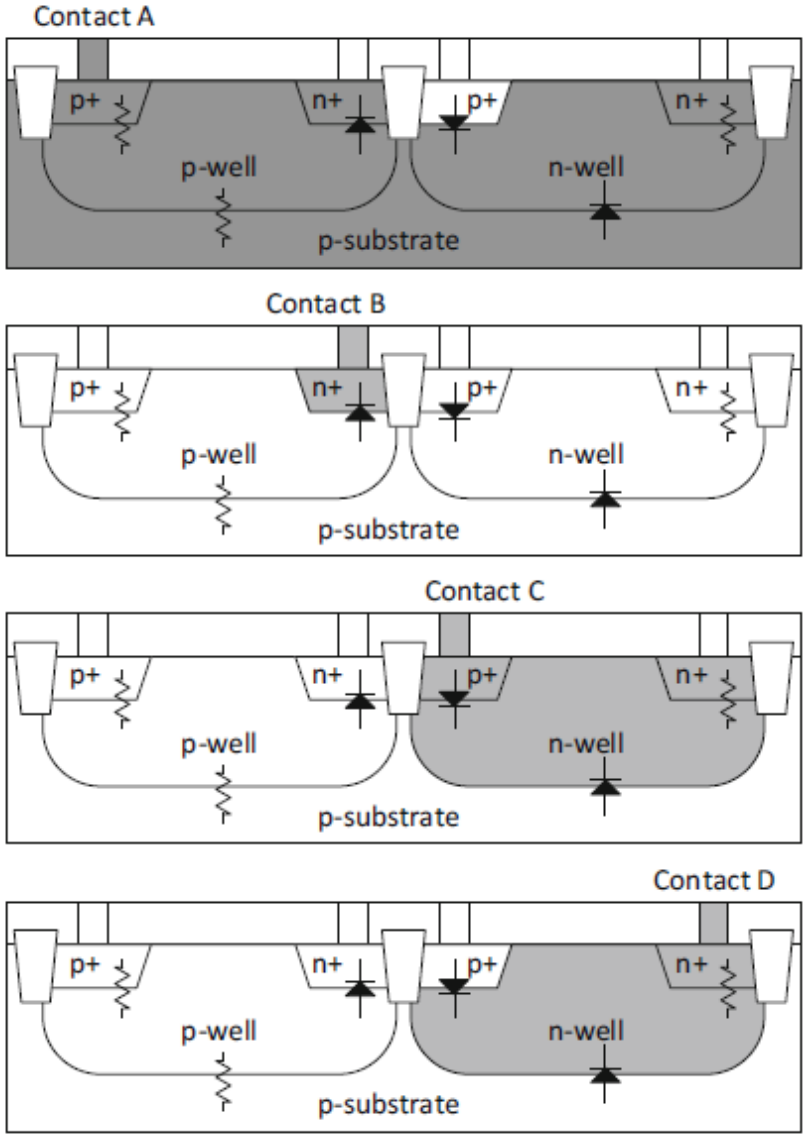


Reversing Stealthy Dopant-level Trojans

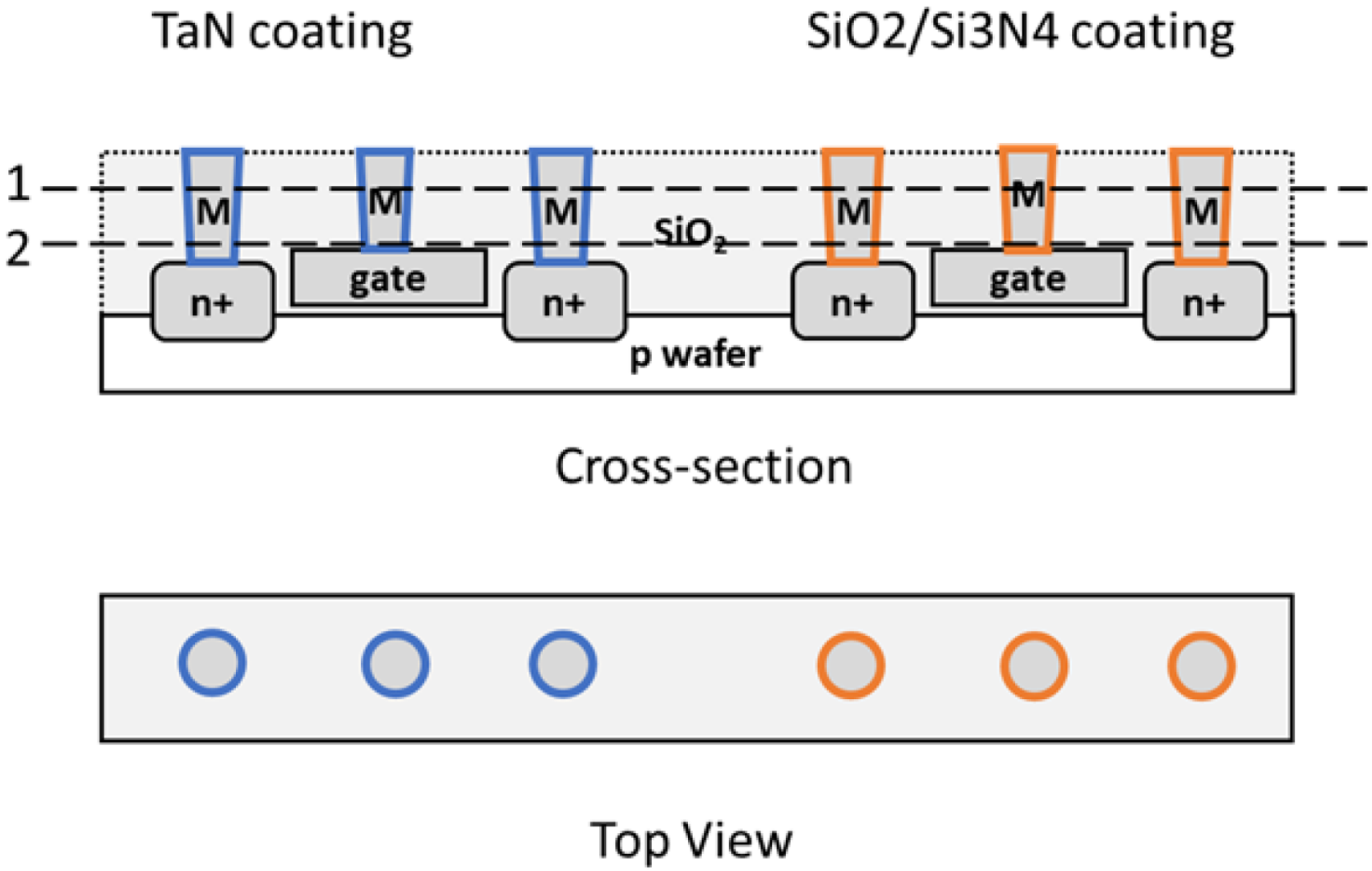
Sugawara et al, CHES 2014

- **Passive Voltage Contrast (PVC)** is a measurement principle used by SEM/FIB to measure surface voltage of a sample
- Dopant configurations used by dopant-level Trojans can be distinguished with PVC even when a chip is measured at power-off state!





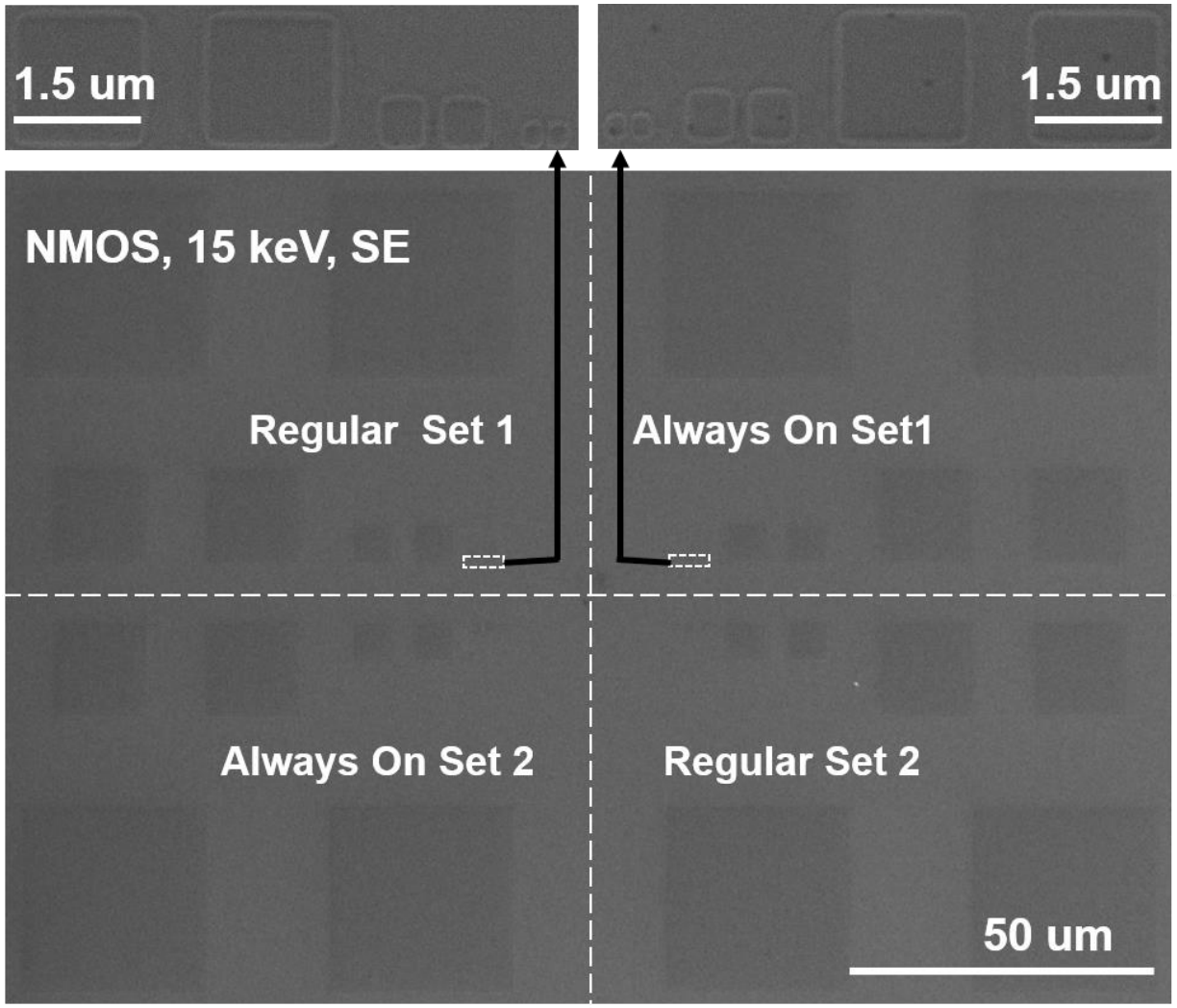
Etching

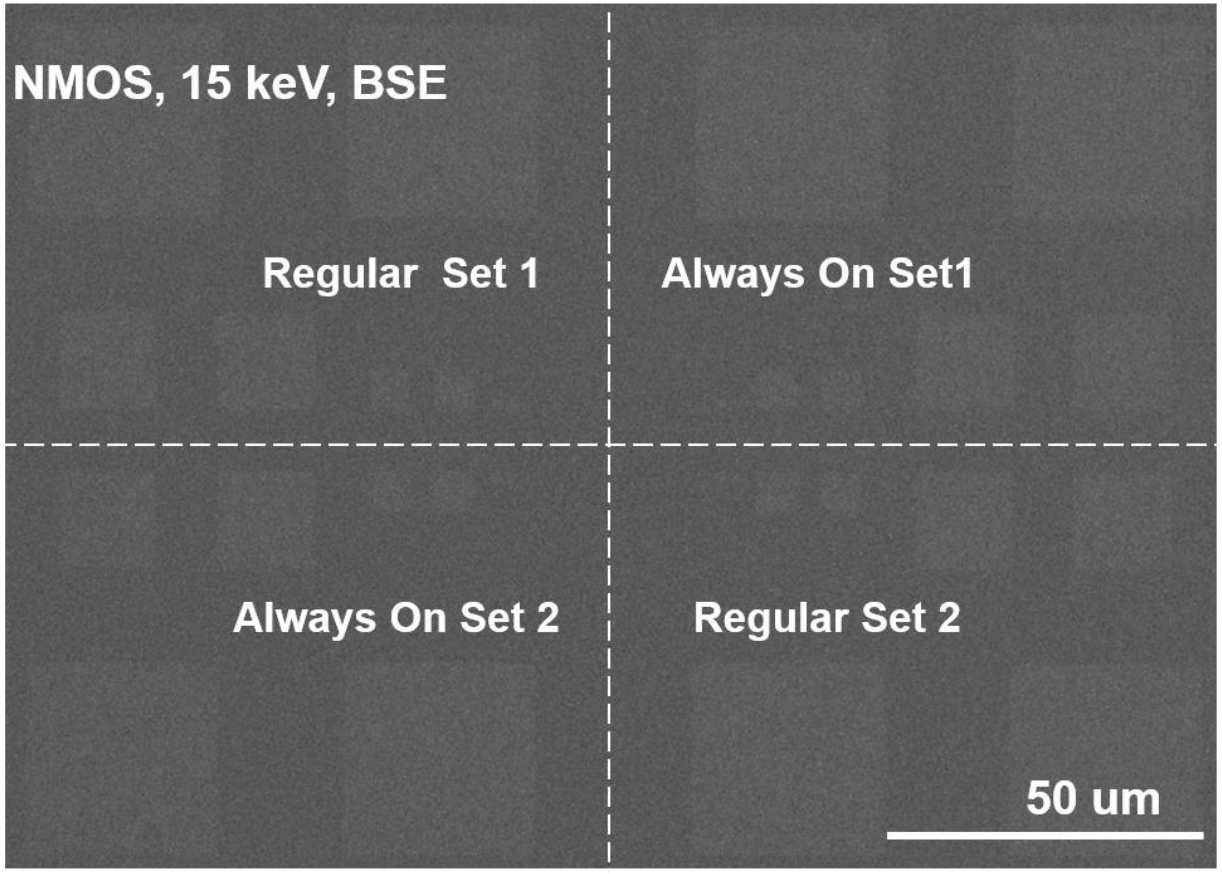

TaN coating
SiO2/Si3N4 coating
1
2
M
M
M
M
M
M
SiO_2
n+
gate
n+
n+
gate
n+
p wafer
Cross-section
Top View

Comparison to Other Camouflaging Techniques

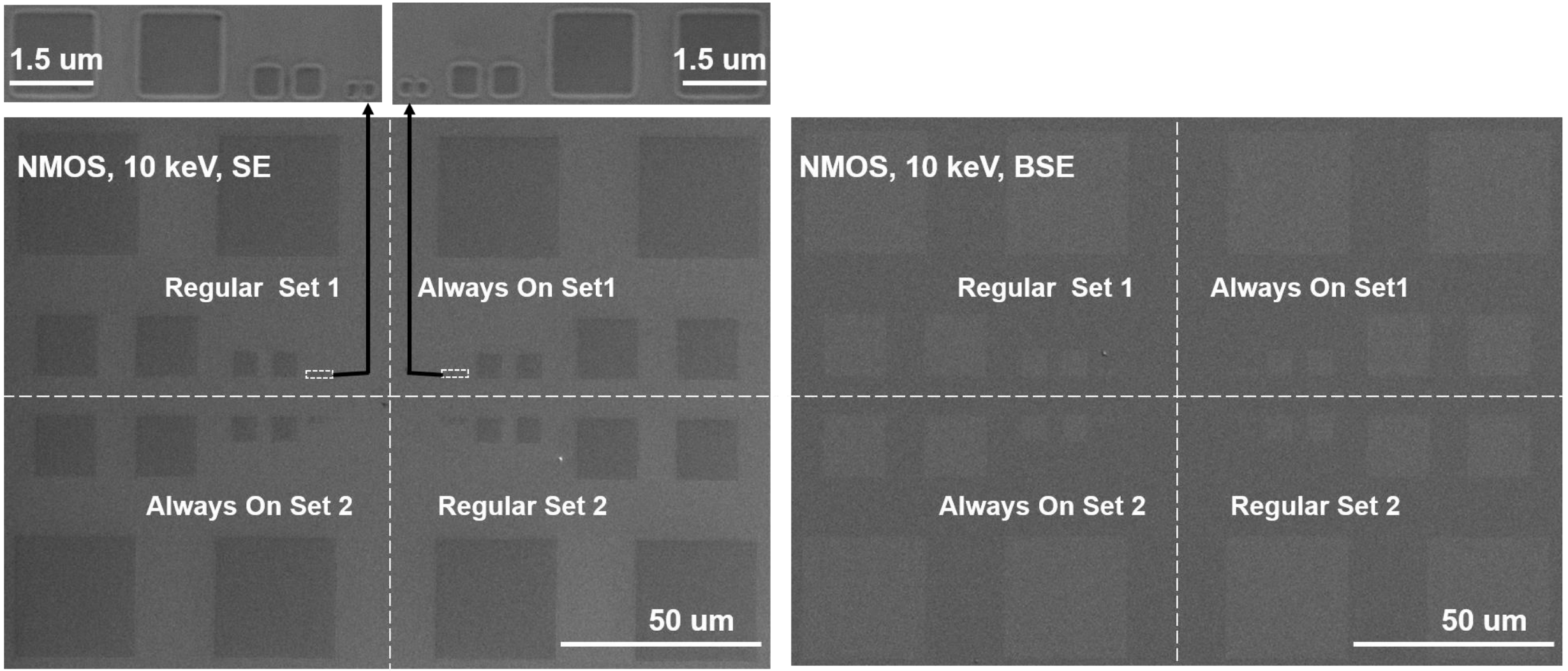
Feature	Regular Camouflaging				Covert Gates
	Dummy Contact	Threshold Voltage	Doping	Transformable Interconnects	
SAT resistant at low overhead	✗	✗	✗	✗	✓
Test attack resistant	✗	✗	✗	✗	✓
Low overhead	✗	✗	✗	✗	✓
Configurable after fabrication	✗	✓	✗	✗	✗
Imaging resistant	✓	✓	✓	?	✓
Undetectable during netlist extraction	✗	✗	✗	✗	✓

SEM Images: NMOS, 15 keV, SE and BSE

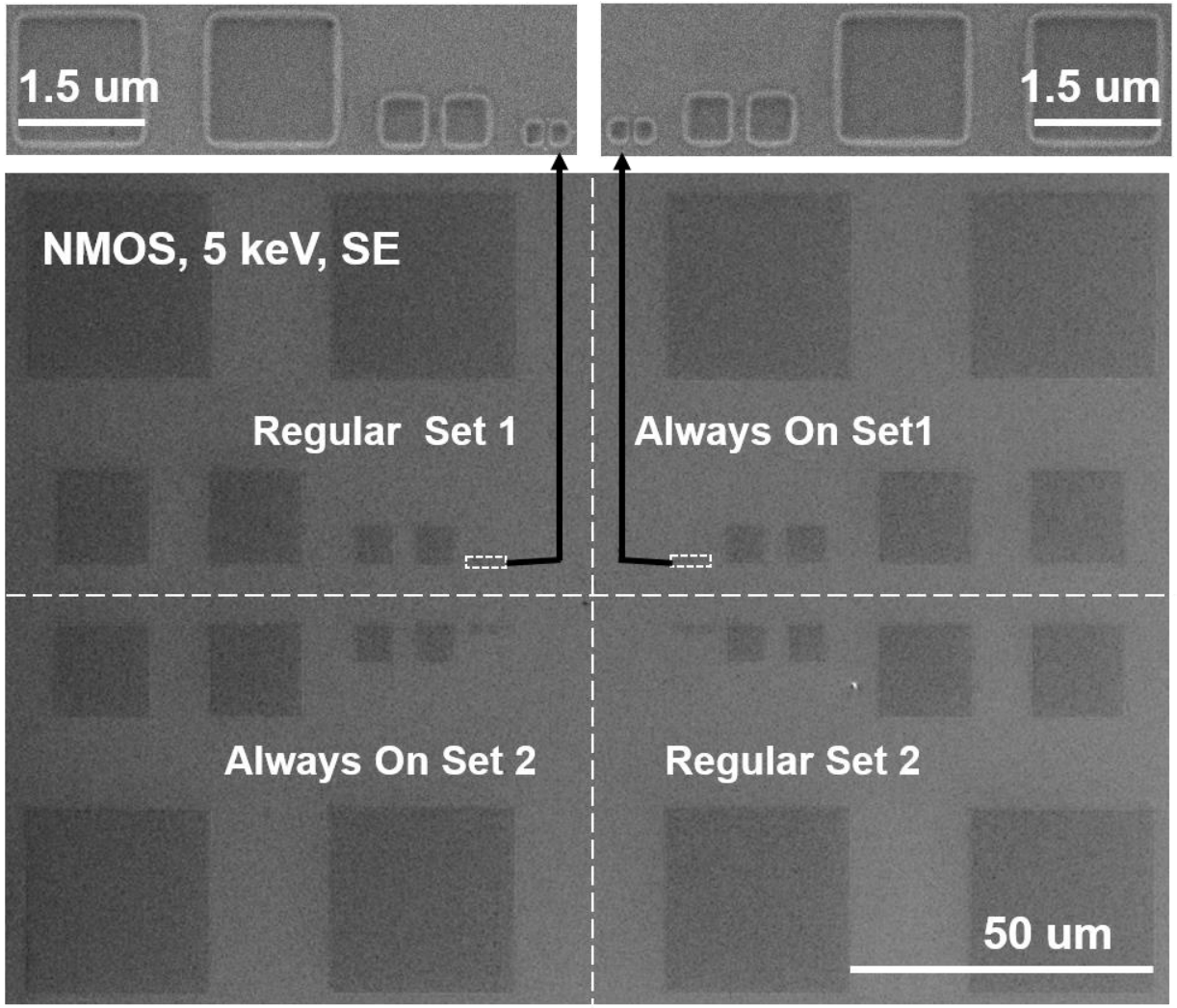


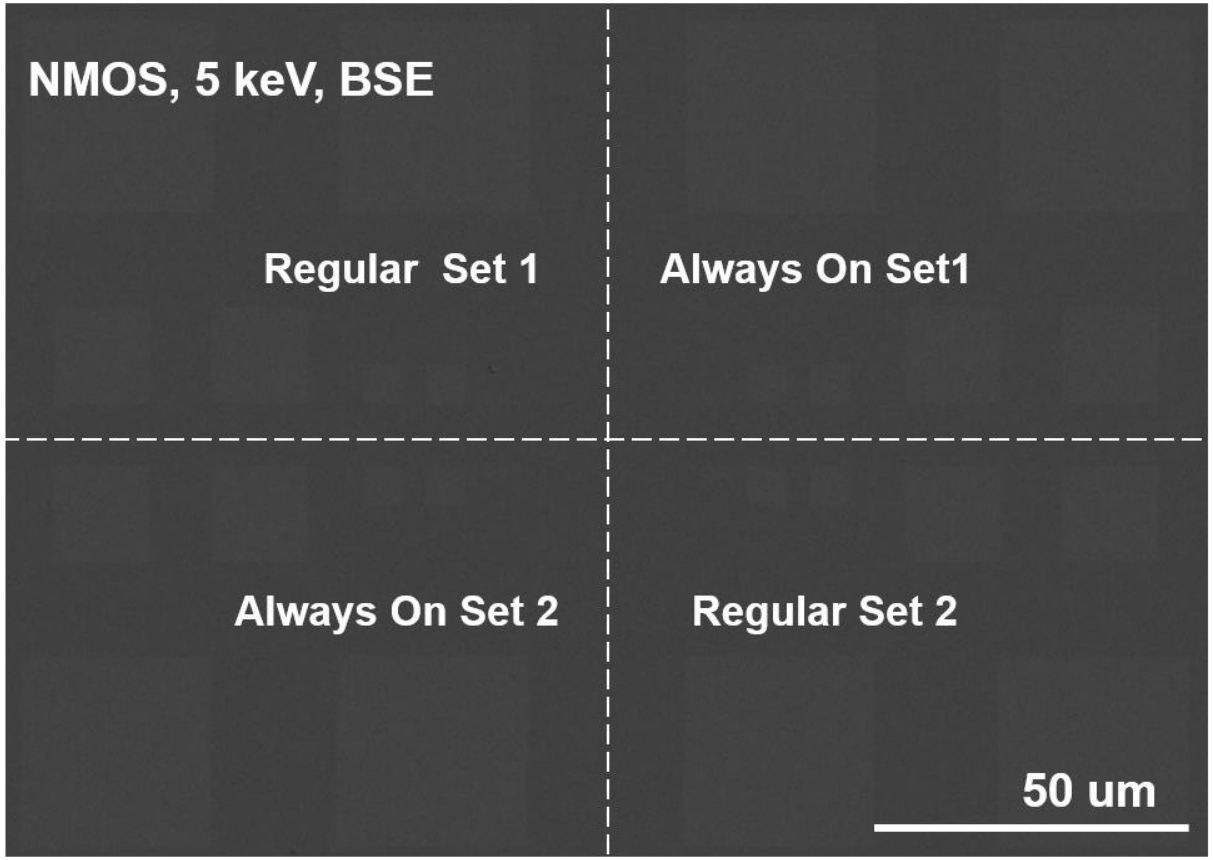


SEM Images: NMOS, 10 keV, SE and BSE

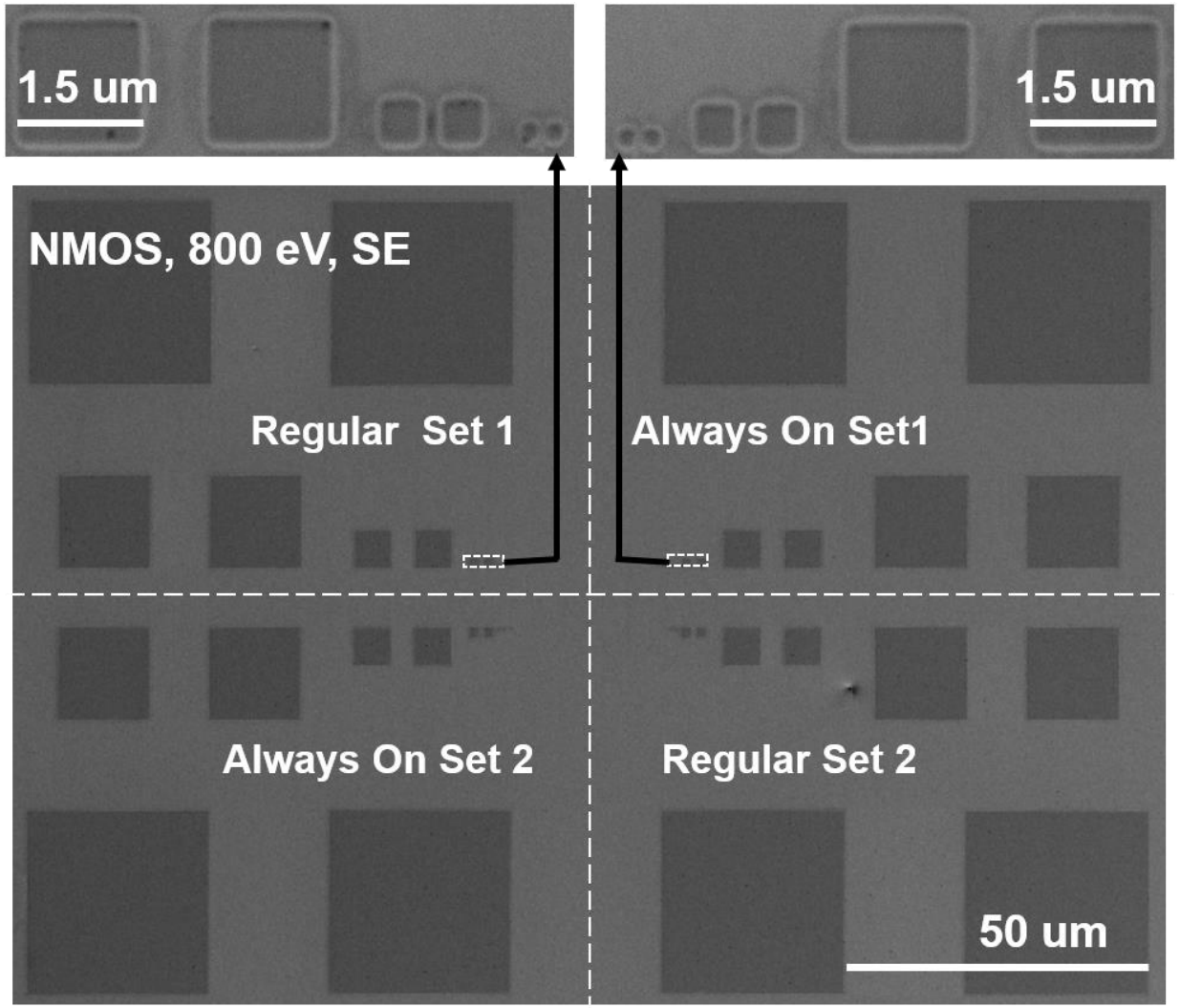


SEM Images: NMOS, 5 keV, SE and BSE



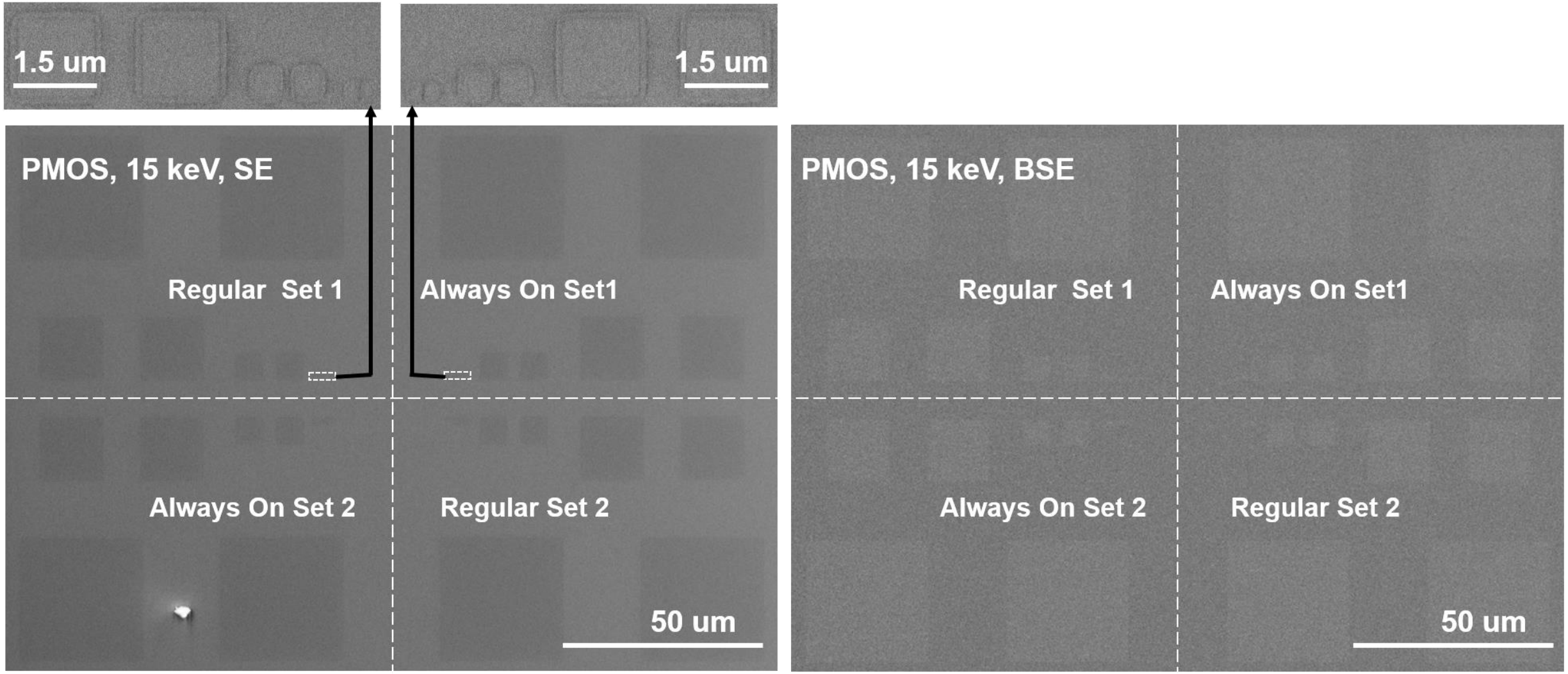


SEM Images: NMOS, 800 eV, SE and BSE

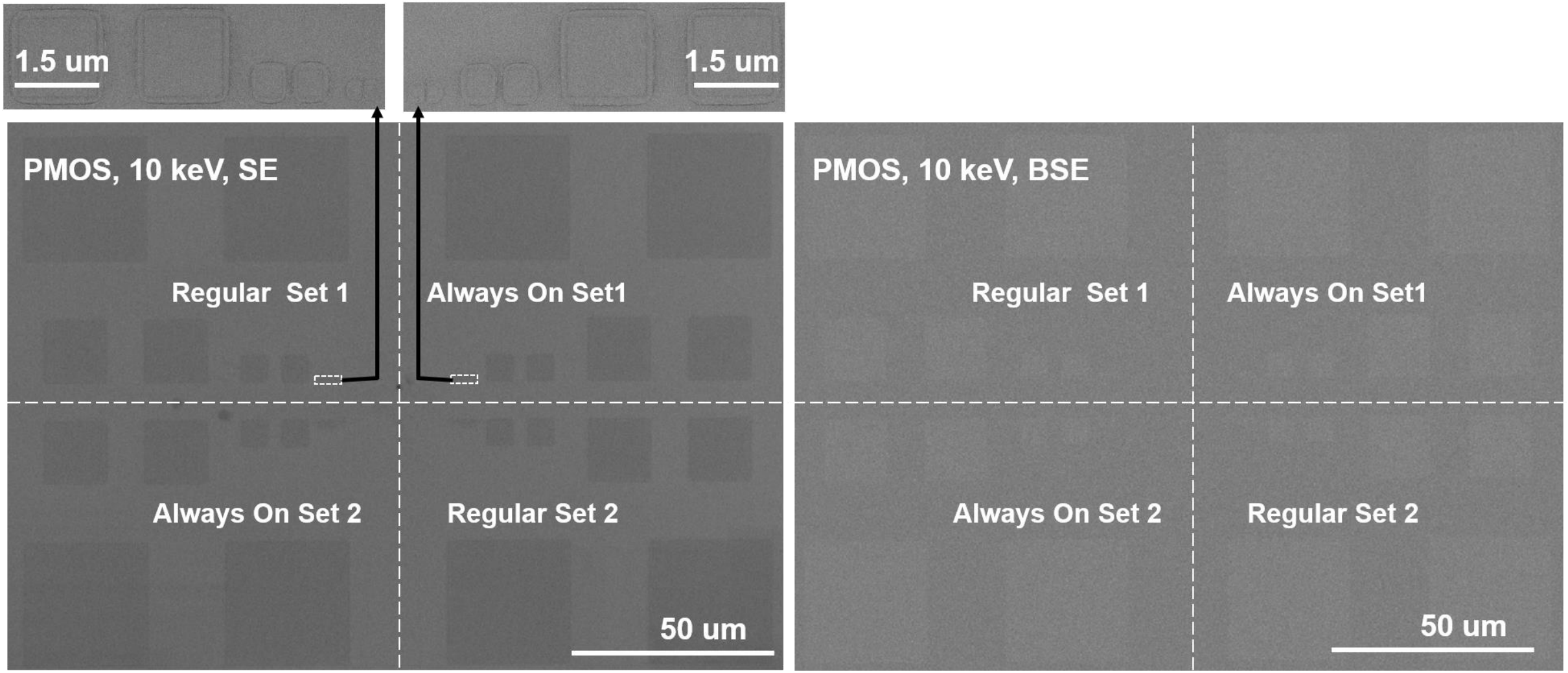


BSE mode is not available with 800eV

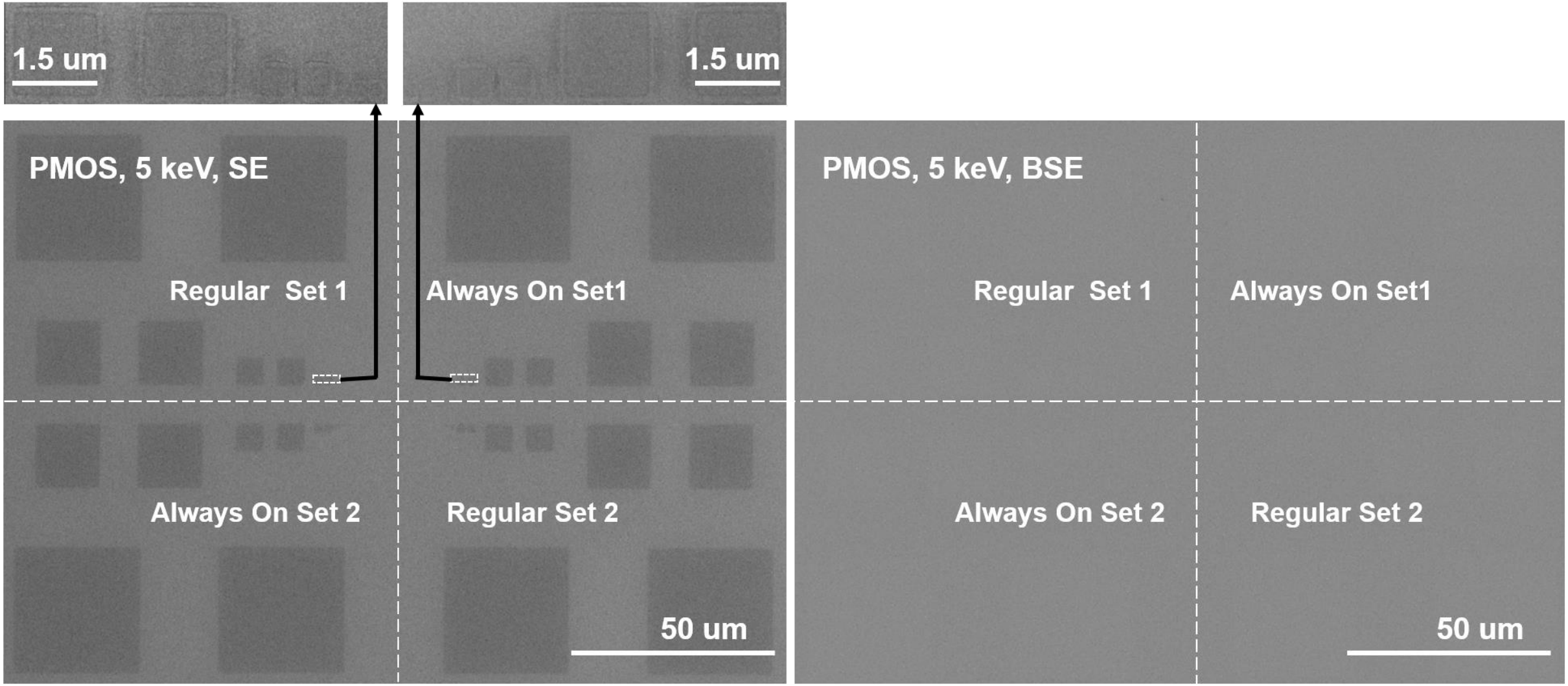
SEM Images: PMOS, 15 keV, SE and BSE



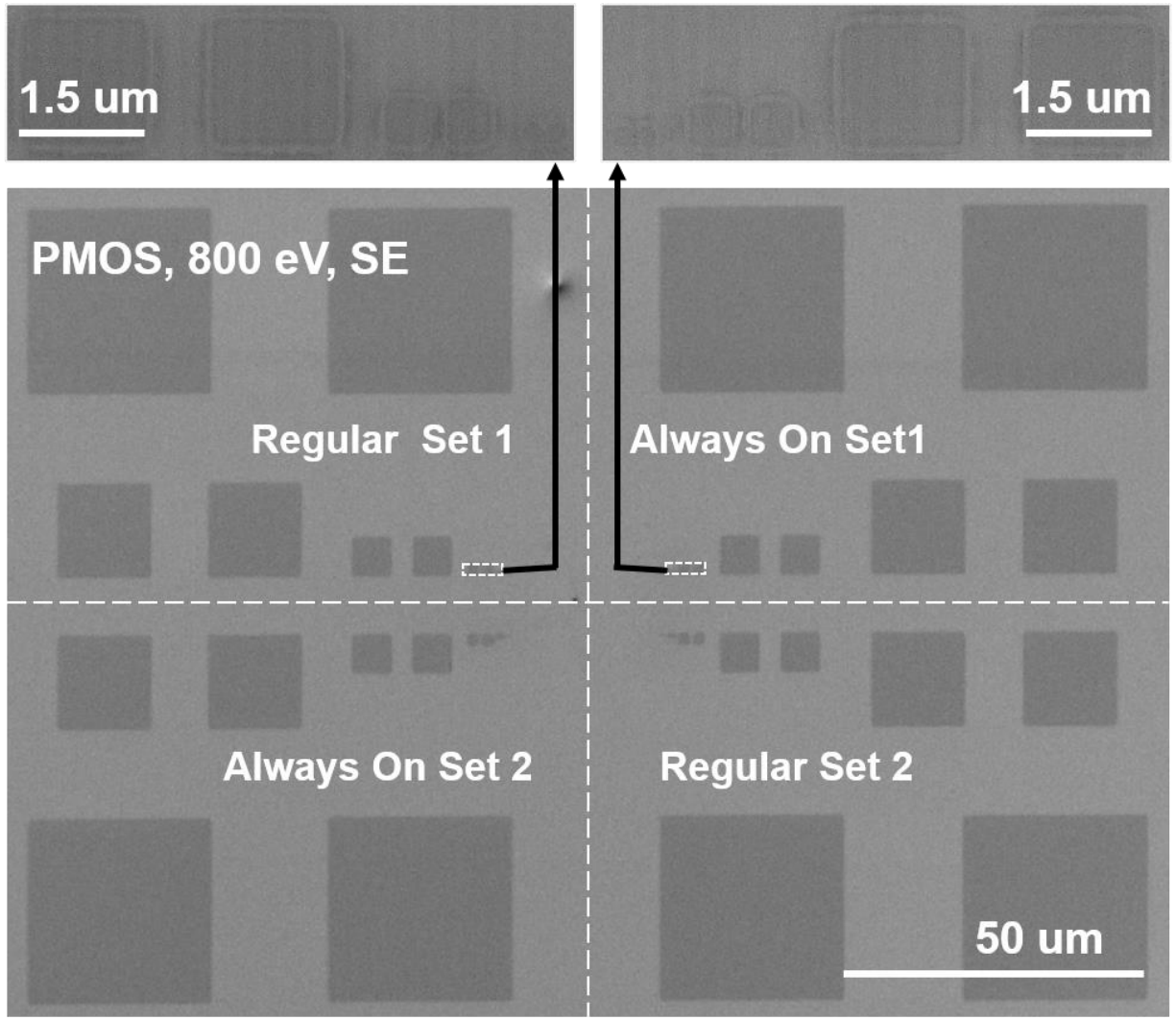
SEM Images: PMOS, 10 keV, SE and BSE



SEM Images: PMOS, 5 keV, SE and BSE



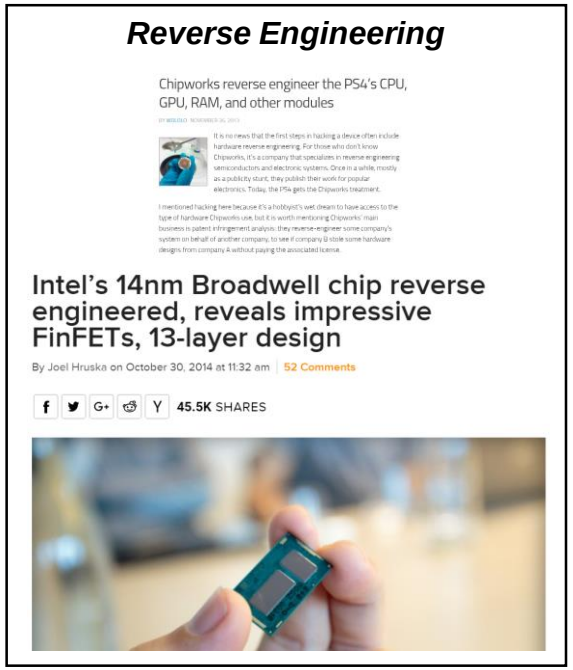
SEM Images: PMOS, 800 eV, SE and BSE



BSE mode is not available with 800eV

IP Issues in the Public Domain

Reverse Engineering



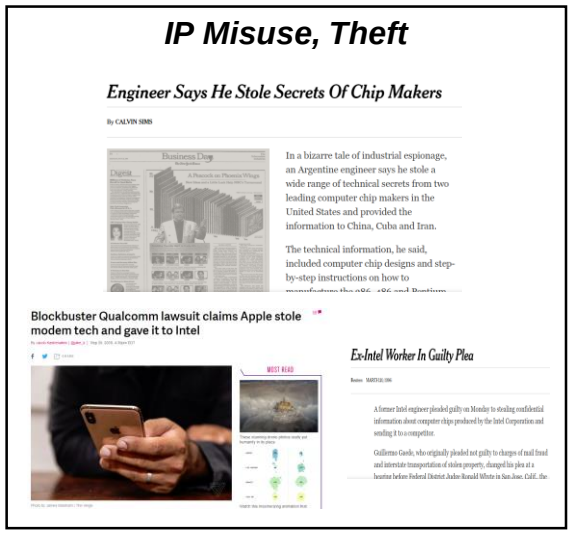
Chipworks reverse engineer the PS4's CPU, GPU, RAM, and other modules

Intel's 14nm Broadwell chip reverse engineered, reveals impressive FinFETs, 13-layer design

By Joel Hruska on October 30, 2014 at 11:32 am | 52 Comments

45.5K SHARES

IP Misuse, Theft



Engineer Says He Stole Secrets Of Chip Makers

Blockbuster Qualcomm lawsuit claims Apple stole modem tech and gave it to Intel

Ex-Intel Worker In Guilty Plea

semi

From the SEMI President and CEO

Innovation is at Risk: Losses of up to $4 Billion Annually due to IP Infringement

Protection of intellectual property (IP) rights is an important area of concern for the semiconductor manufacturing industry. In a competitive global business environment, IP protection is essential to the survival of equipment and materials suppliers, enabling them to invest the significant R&D funds needed to sustain technological advancement of the semiconductor industry.

In recent years, suppliers have been increasingly funding a larger portion of the escalating R&D costs needed for the continued success of the semiconductor device industry. These challenging conditions pose a serious thre… …cs supply chain, where IP has alw… …tinued IP violations of various forr… …t generation equipment and ma… …aw technology curve.

In re… …orts in protection and enforcement of IP ri… …udy on the extent and impact of IP cha… …on the survey findings, is now

The Register®
Biting the hand that feeds IT

Security

Boffins deduce chip's crypto just by looking at it

Smartcard hacking enters script-kiddie phase

By Dan Goodin 4 Aug 2011 at 04:35 19 SHARE

Black Hat Hackers have released tools that unlock the software stored on heavily fortified chips so researchers can independently assess their security and spot weaknesses.

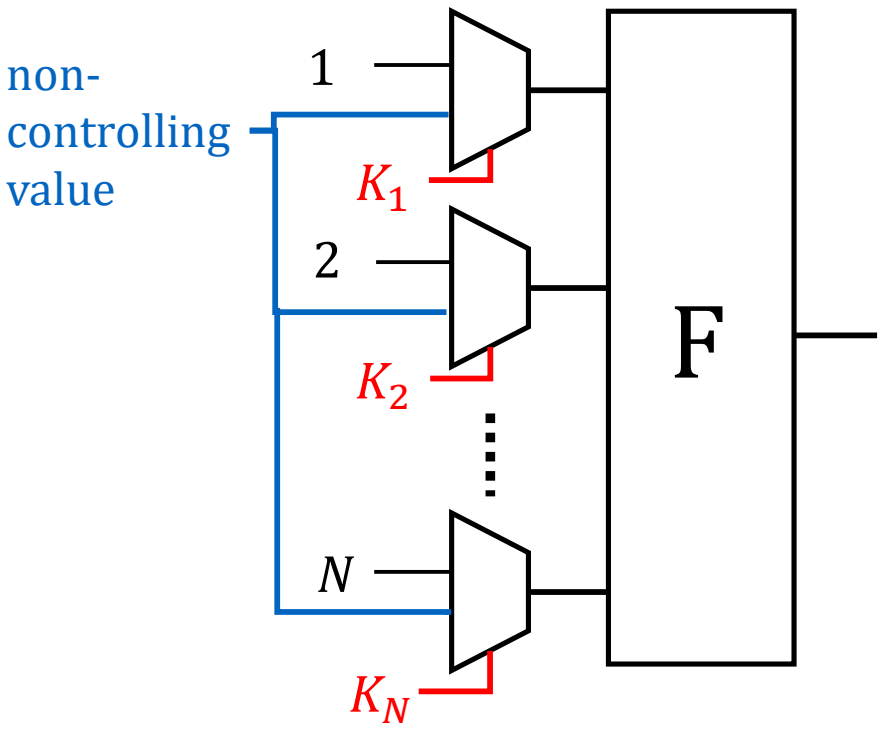
At the heart of the the release, which was announced Wednesday at the Black Hat Security conference in Las Vegas, is Degate, software developed by Martin Schobert for hardware experts to analyze small silicon structures. It has recently been refined so it can be used by

…zed semiconductor supply …ds to the possibility of **IP …e and compromise** *at …very stage*.

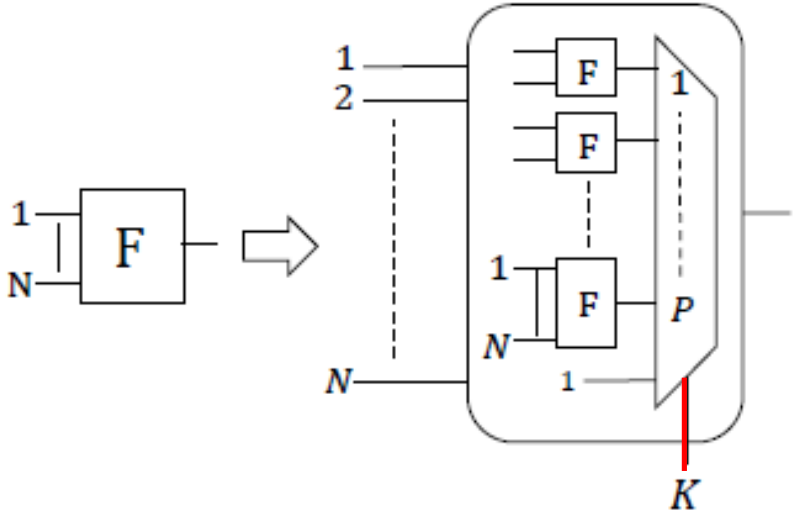
…equences range from lost …ue to design tampering.

…backbone of every chip …nd needs ***active …on mechanisms*** at various … abstraction in the supply

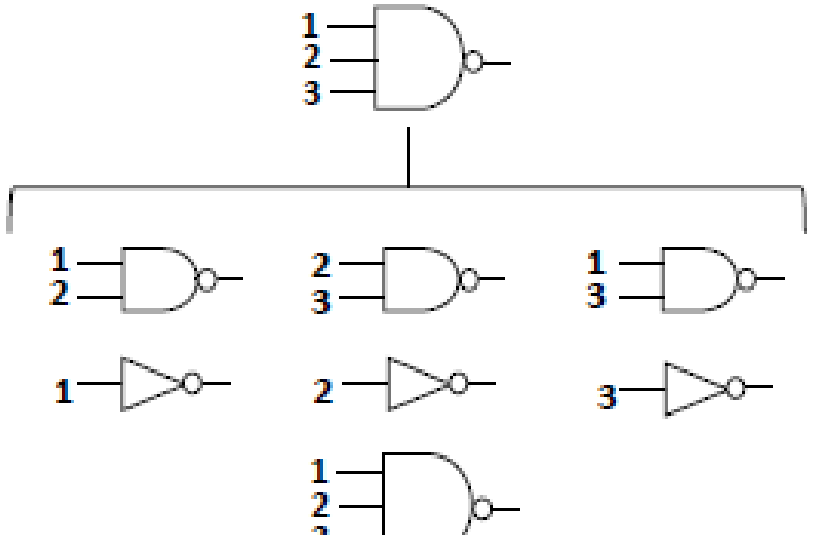
SAT Attack Formulation on Covert Gates



- Correct key chooses correct pin permutation network



-



gates

l form (CNF)

n space

Device Structure and Fabrication of Covert Gates