Invasive PUF Analysis

Dmitry Nedospasov Clemens Helfmeier
Jean-Pierre Seifert Christian Boit
Technische Universität Berlin
Chair for Security in Telecommunications (SECT) and
Chair for Semiconductor Devices (HLB)

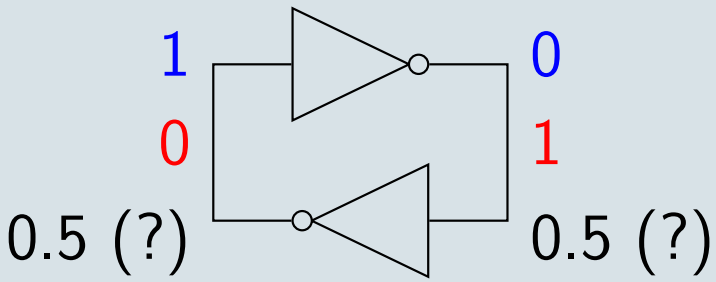
Fault Diagnosis and Tolerance in Cryptography

Helmholtz Research School on Security Technologies

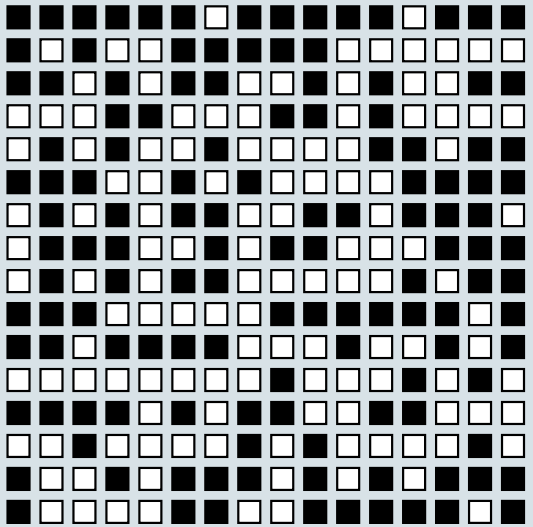
picture by Wikimedia/John L. Wiley `http://flickr.com/jw4pix`

SRAM PUF – basic idea

SRAM cell logic:



possible result:



Apply power to SRAM,
inverters get compared.

PUF response generated

- noise background makes error correction required
- SRAM is already built-in to most devices

The Clone SRAM Procedure – Episode I

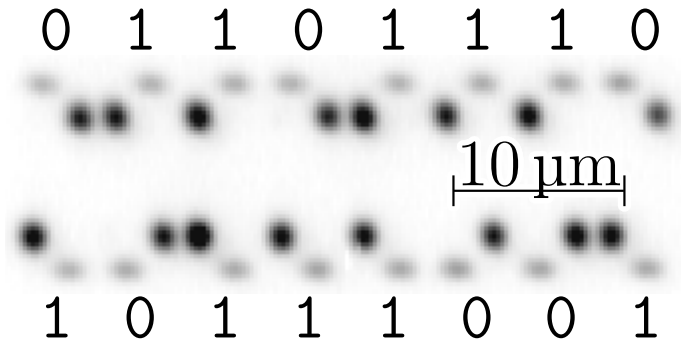
1. **Characterization**

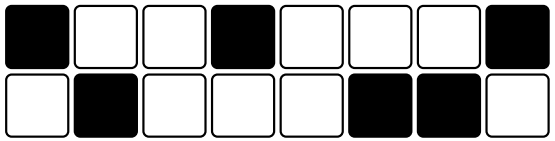
2. **Manufacturing**

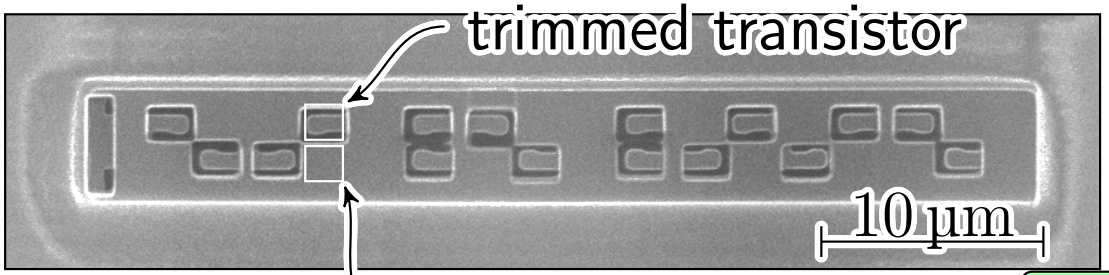
(HOST 2013)

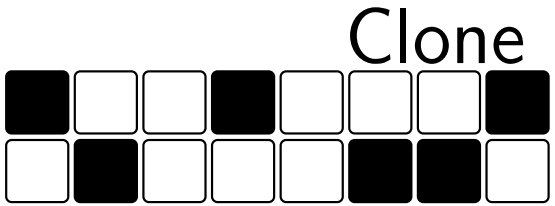
picture by Wikimedia/Eva Rinaldi

Backside FIB trimming







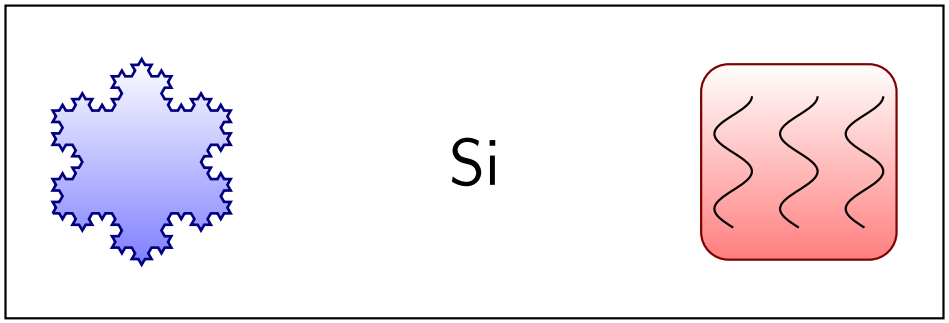


memory fully functional

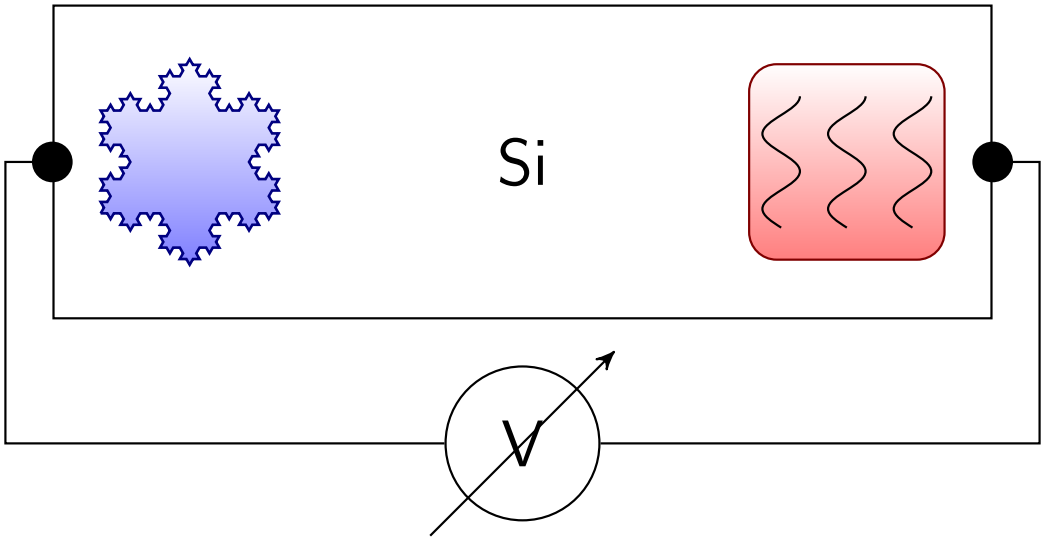
C. Helfmeier et. al., HOST 2013: Cloning Physically Unclonable Functions

Overview

The Seebeck Effect



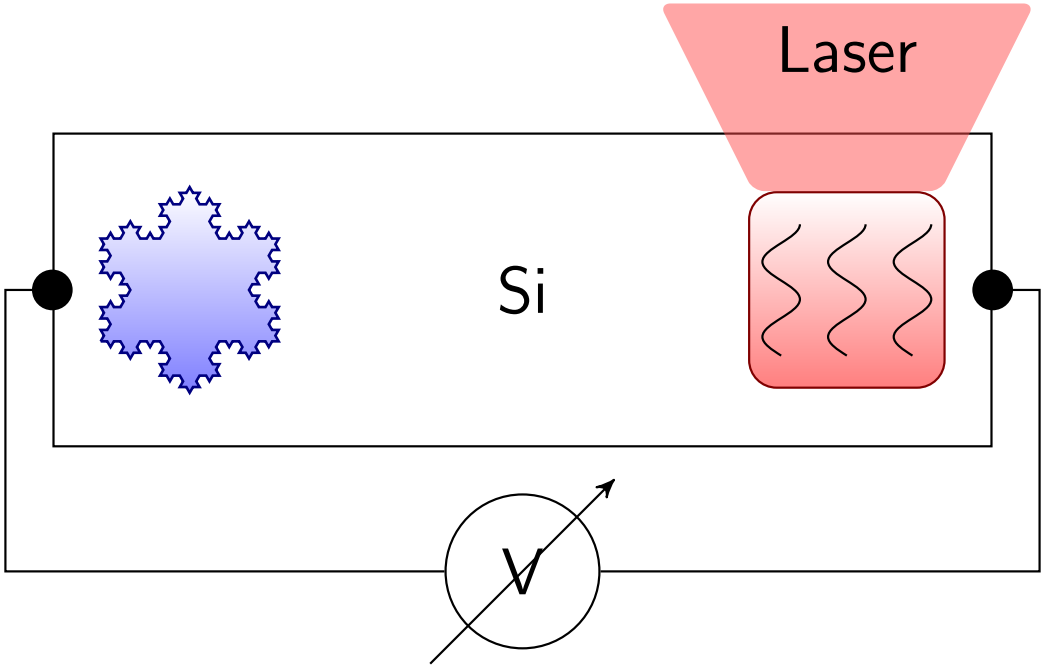
The Seebeck Effect



$$V_{\text{Seebeck}} = \alpha \Delta T$$

- α is the Seebeck coefficient.
- α_{metal}: $0.001\,\text{mV}\,\text{K}^{-1}$ to $0.01\,\text{mV}\,\text{K}^{-1}$
- α_{silicon}: $0.2\,\text{mV}\,\text{K}^{-1}$ to $0.4\,\text{mV}\,\text{K}^{-1}$

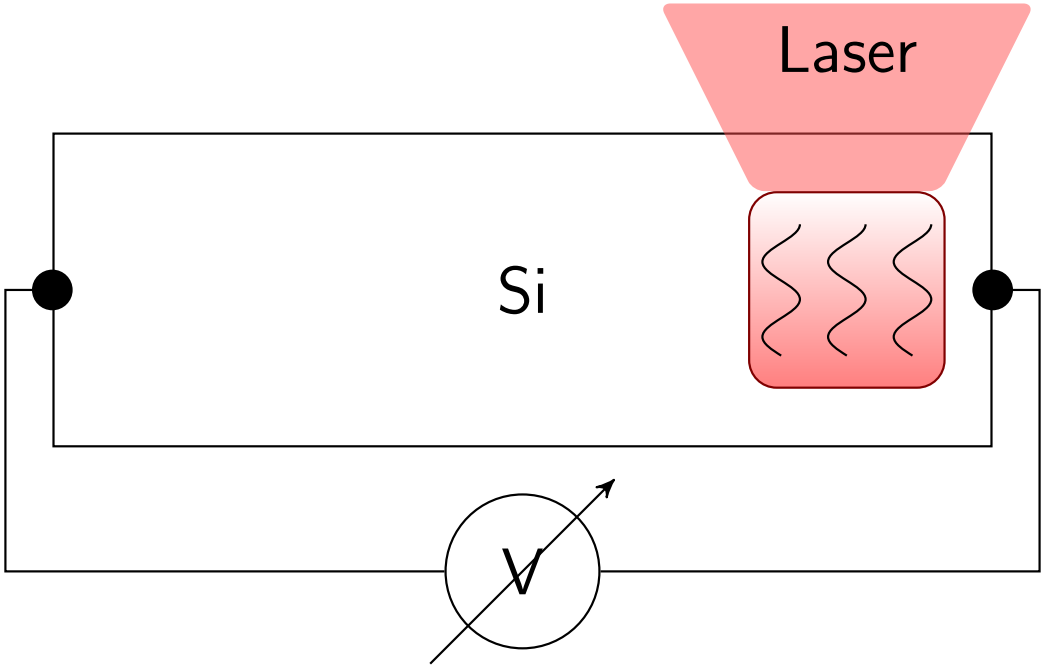
The Seebeck Effect



$$V_{\text{Seebeck}} = \alpha \Delta T$$

- α is the Seebeck coefficient.
- α_{metal}: $0.001\,\text{mV}\,\text{K}^{-1}$ to $0.01\,\text{mV}\,\text{K}^{-1}$
- α_{silicon}: $0.2\,\text{mV}\,\text{K}^{-1}$ to $0.4\,\text{mV}\,\text{K}^{-1}$

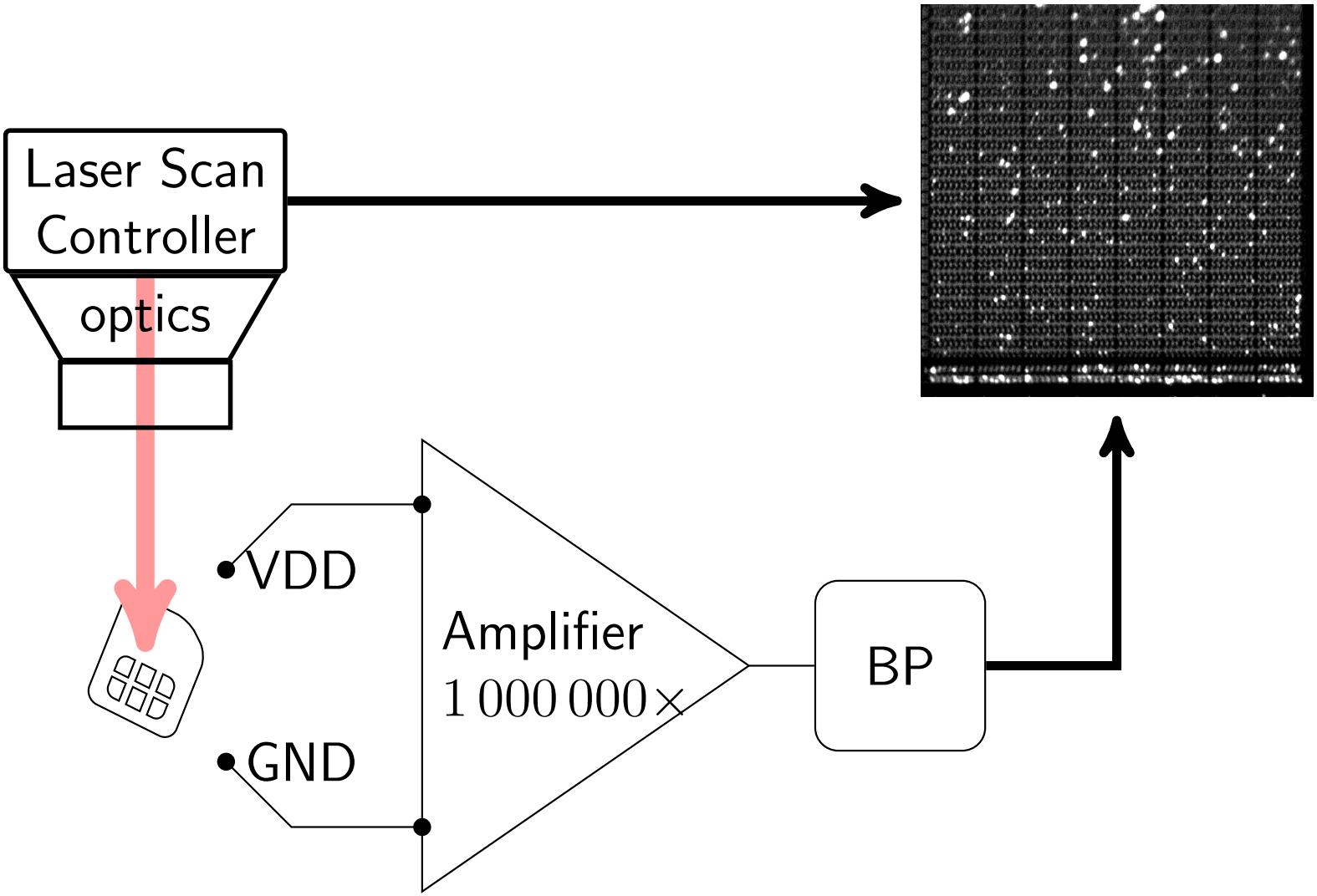
The Seebeck Effect



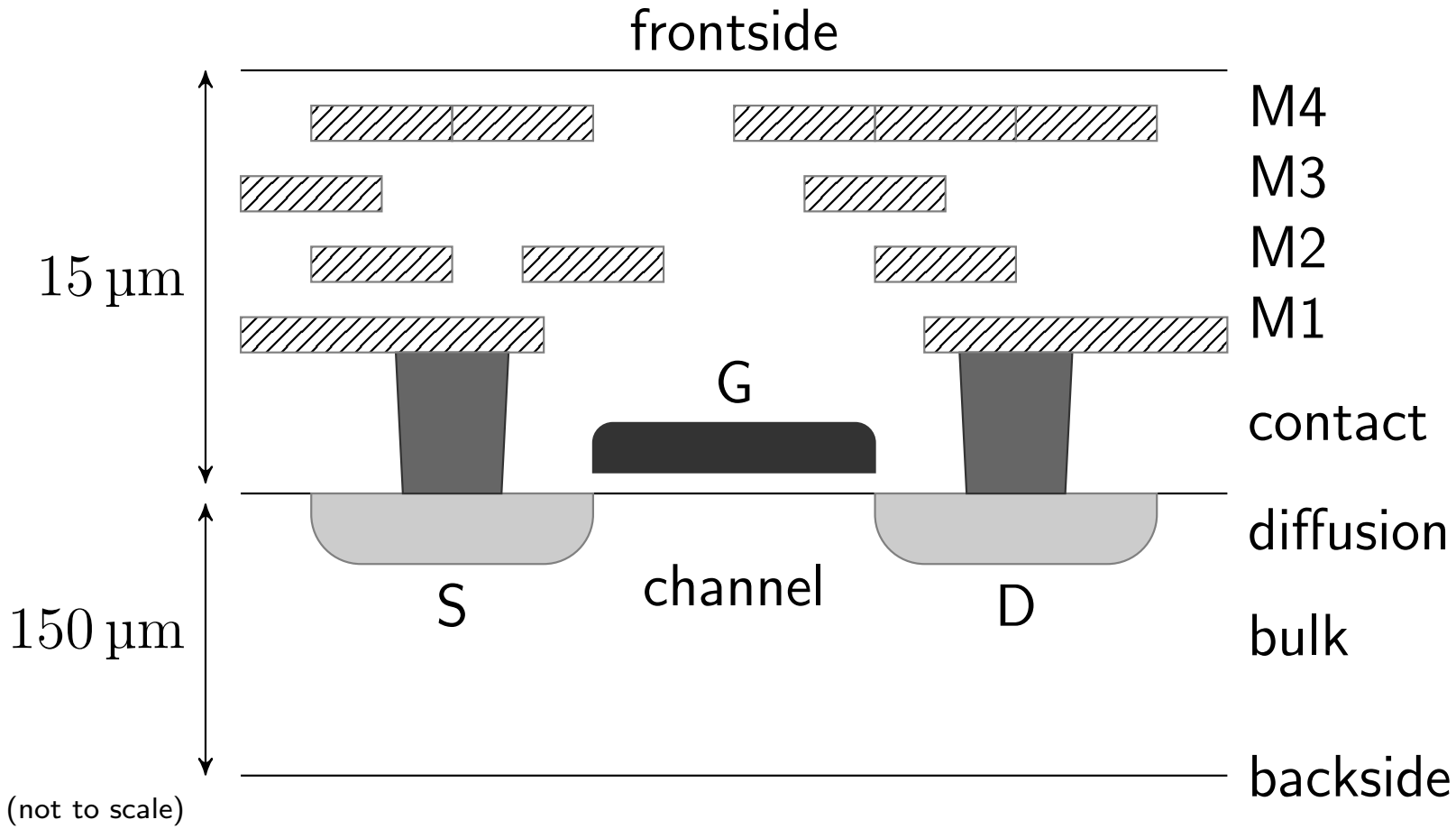
$$V_{\text{Seebeck}} = \alpha \Delta T$$

- α is the Seebeck coefficient.
- α_{metal}: $0.001\,\text{mV}\,\text{K}^{-1}$ to $0.01\,\text{mV}\,\text{K}^{-1}$
- α_{silicon}: $0.2\,\text{mV}\,\text{K}^{-1}$ to $0.4\,\text{mV}\,\text{K}^{-1}$

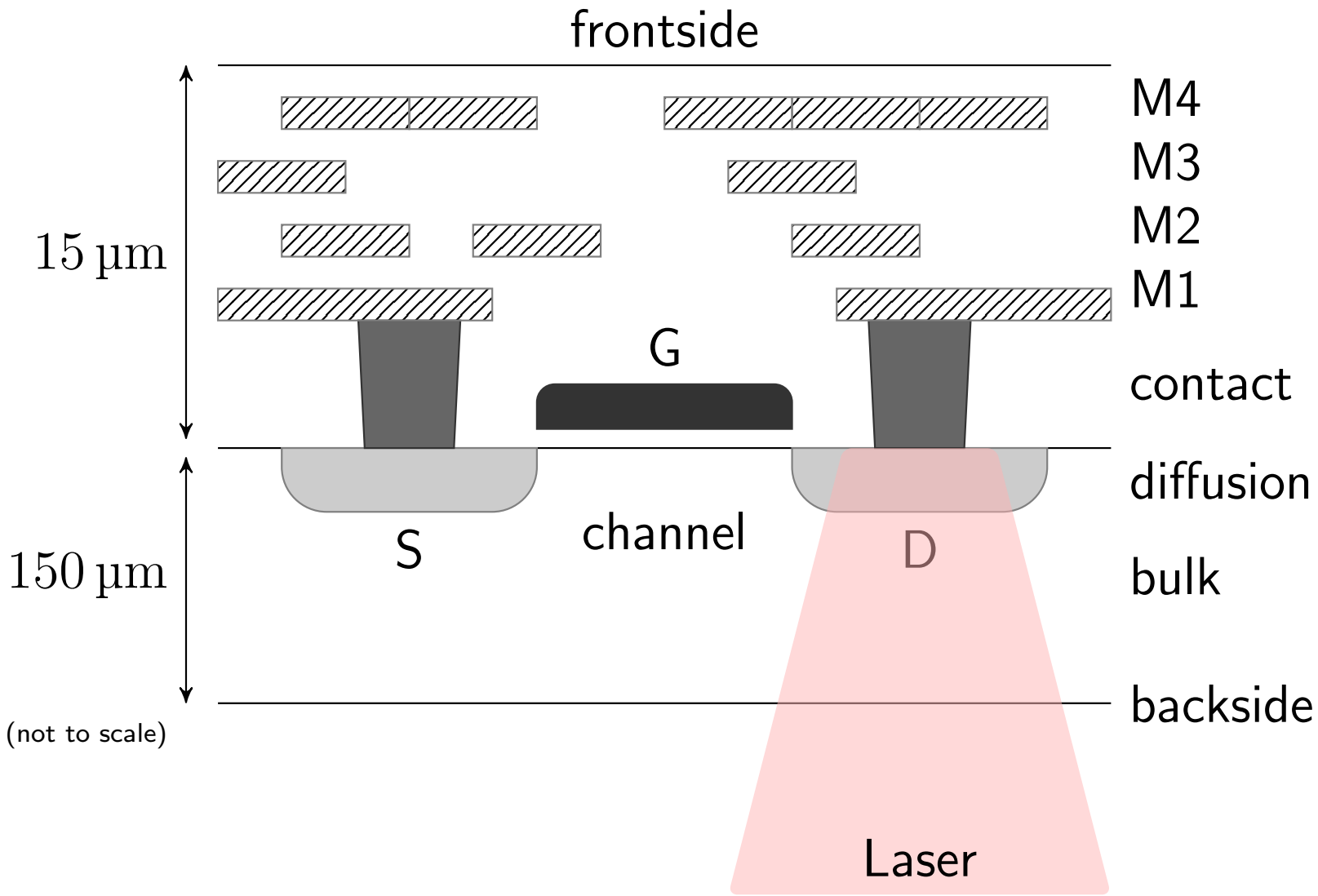
Experimental Setup



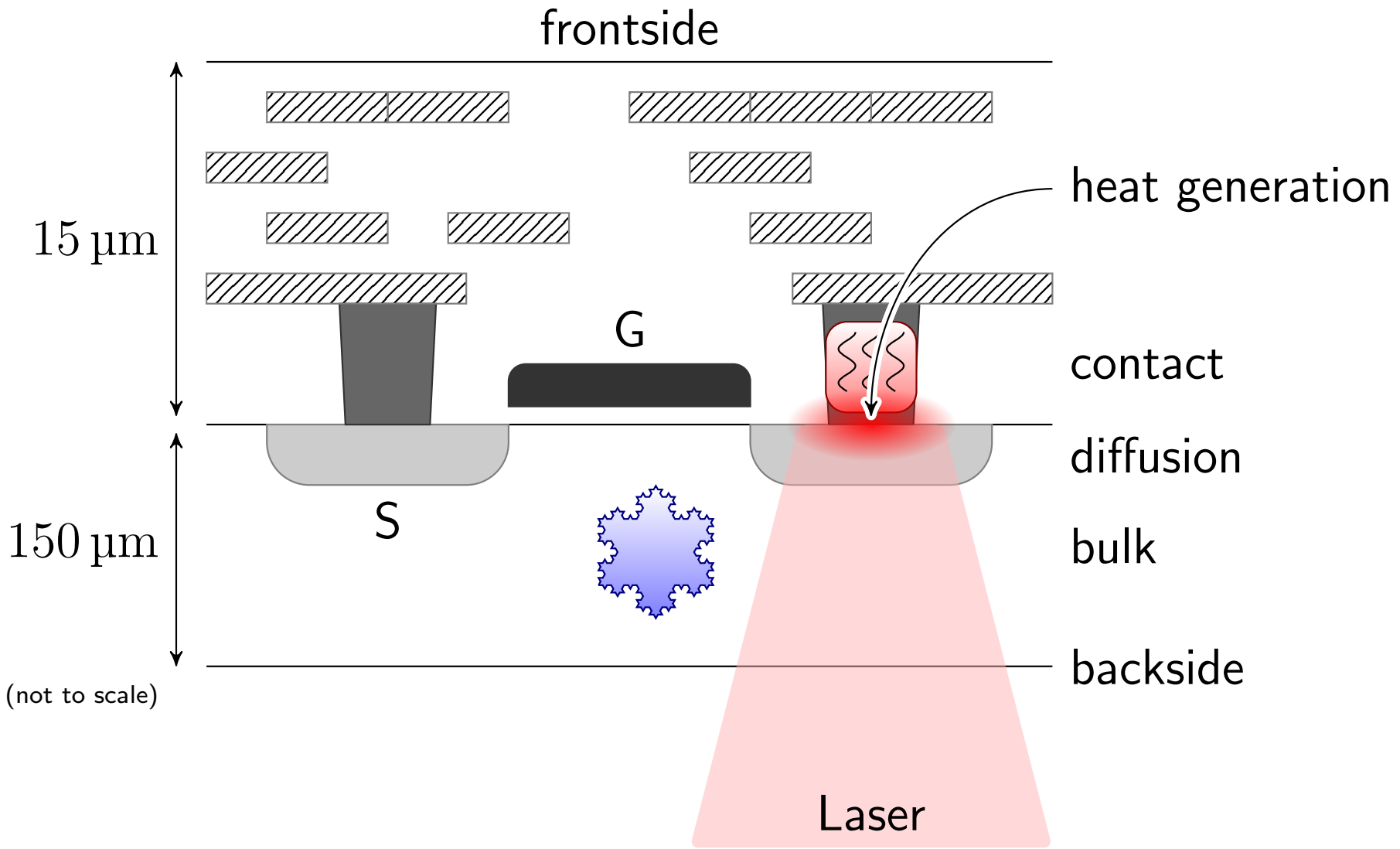
Seebeck Effect on CMOS Transistors



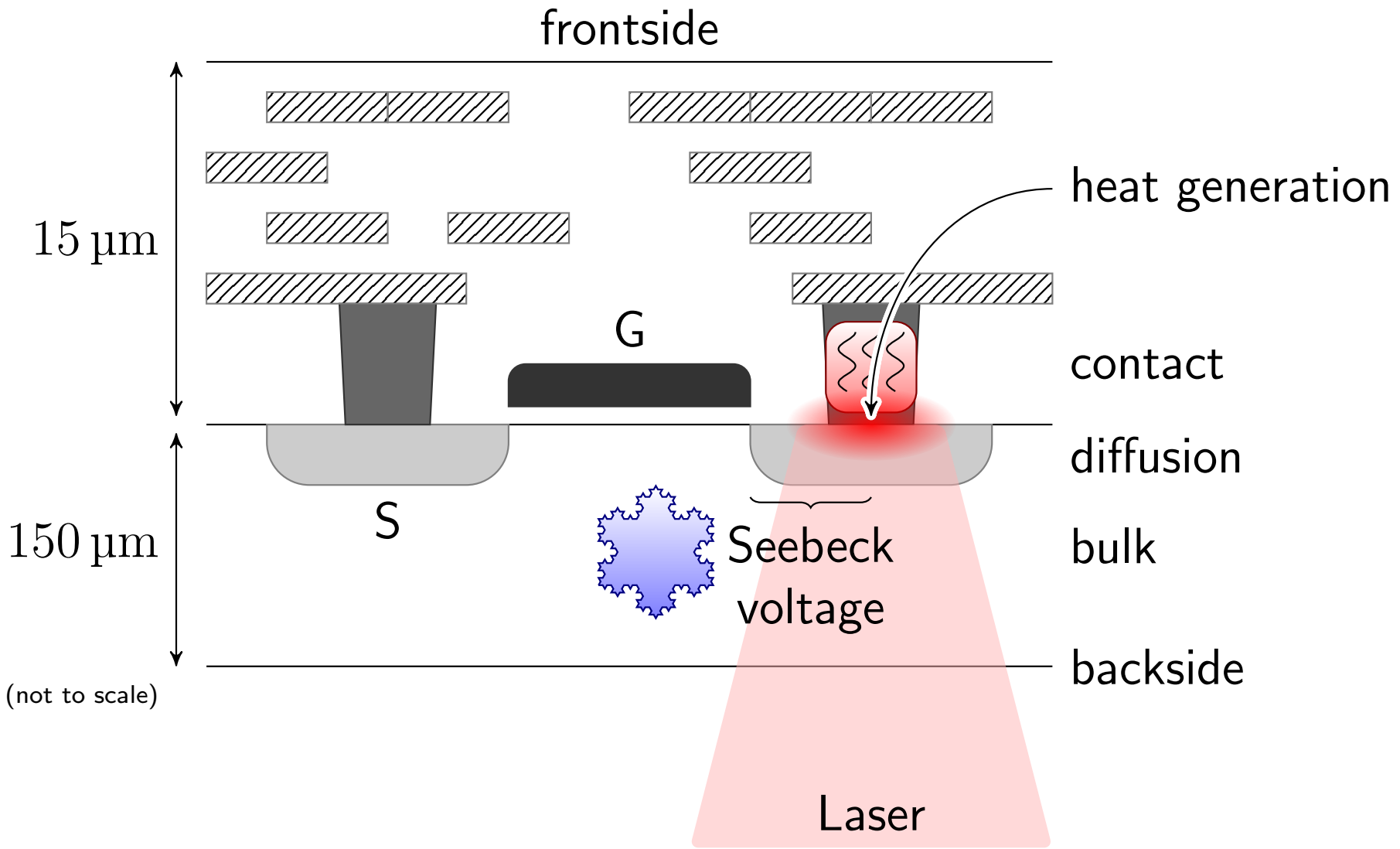
Seebeck Effect on CMOS Transistors



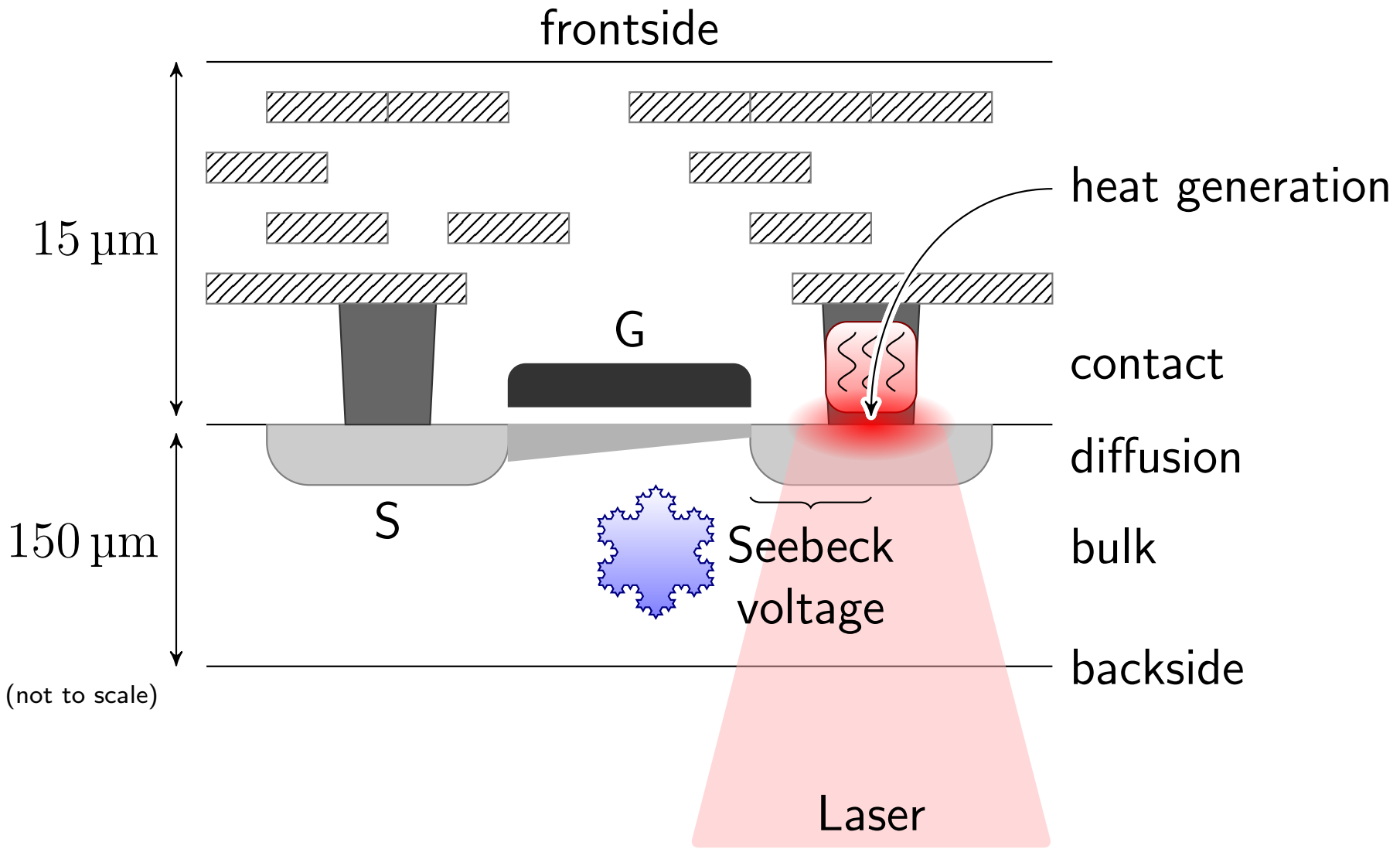
Seebeck Effect on CMOS Transistors



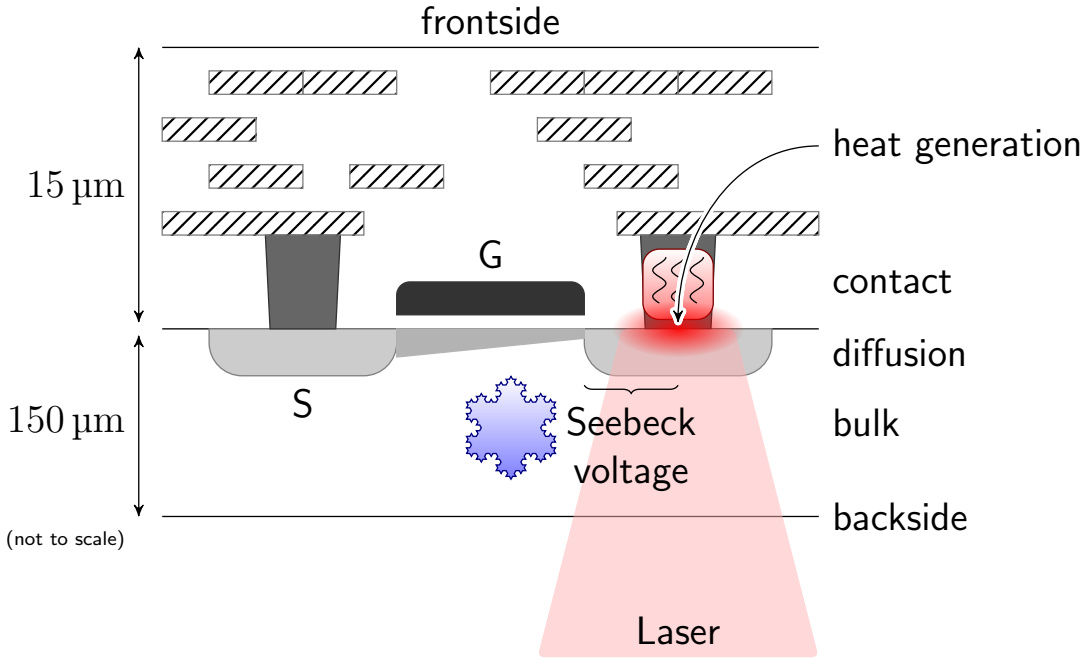
Seebeck Effect on CMOS Transistors



Seebeck Effect on CMOS Transistors

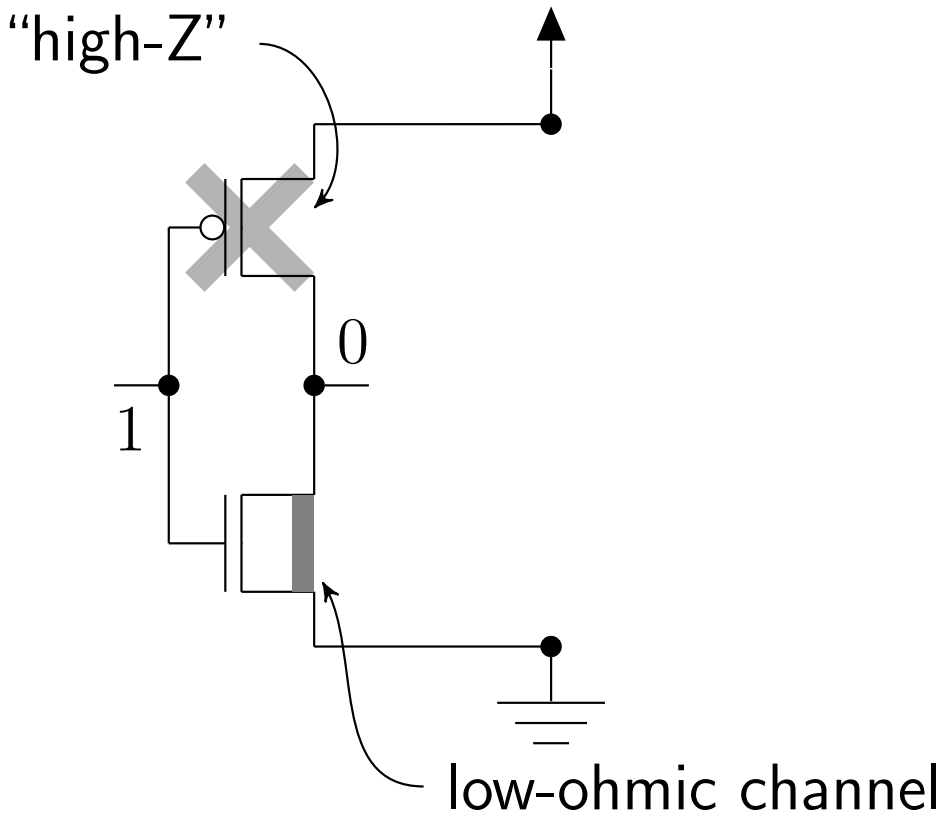


Seebeck Effect on CMOS Transistors

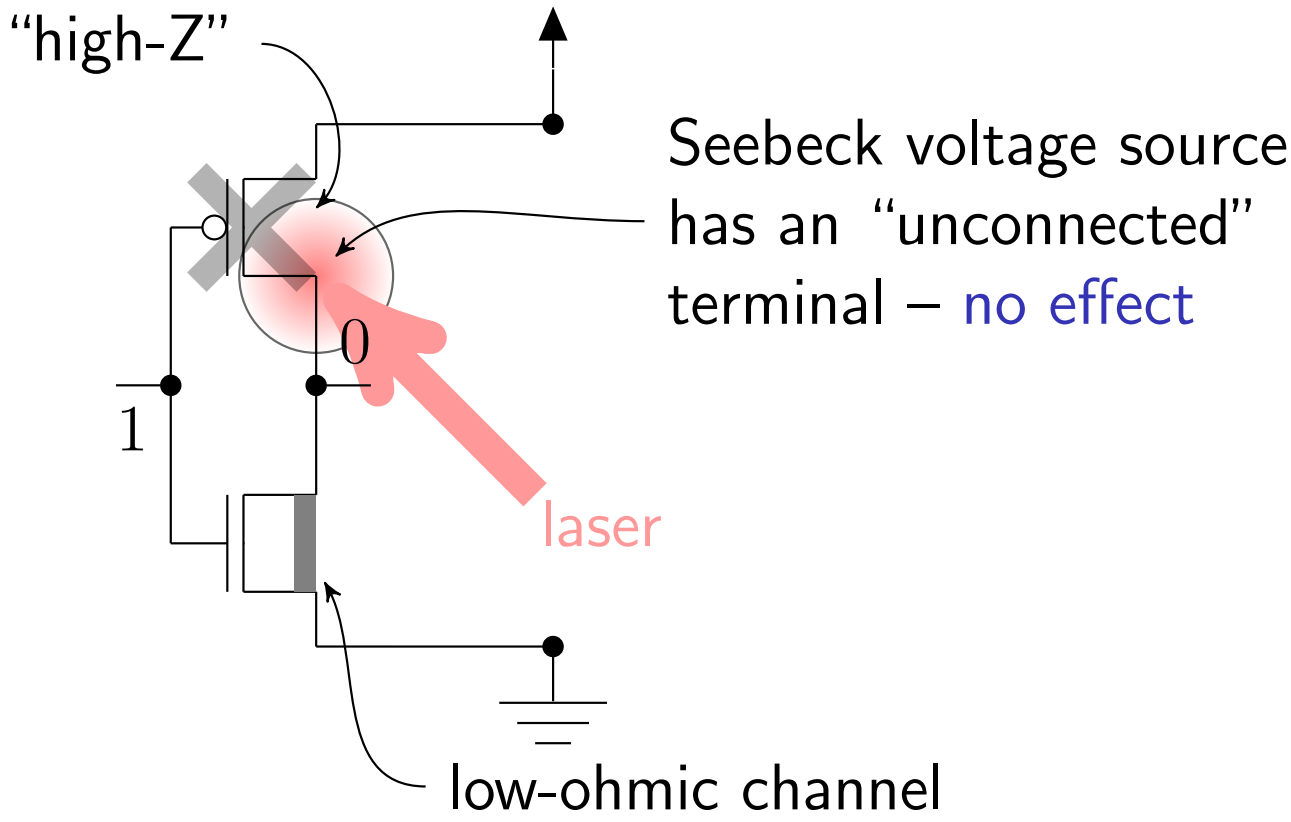


- absorption at source and drain significant
- large Seebeck voltage generated only in silicon
- additional voltage generated at illuminated drain contacts

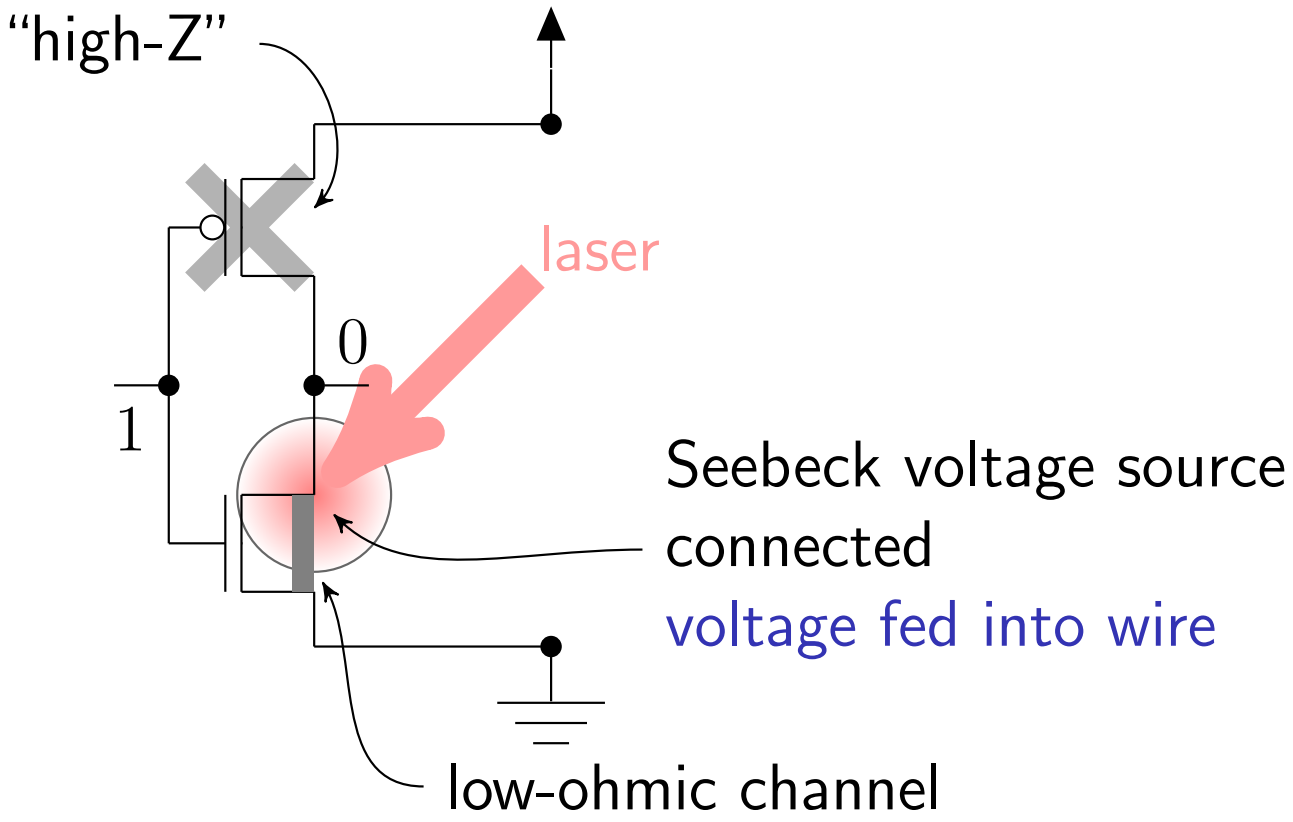
Seebeck Effect on CMOS Gates



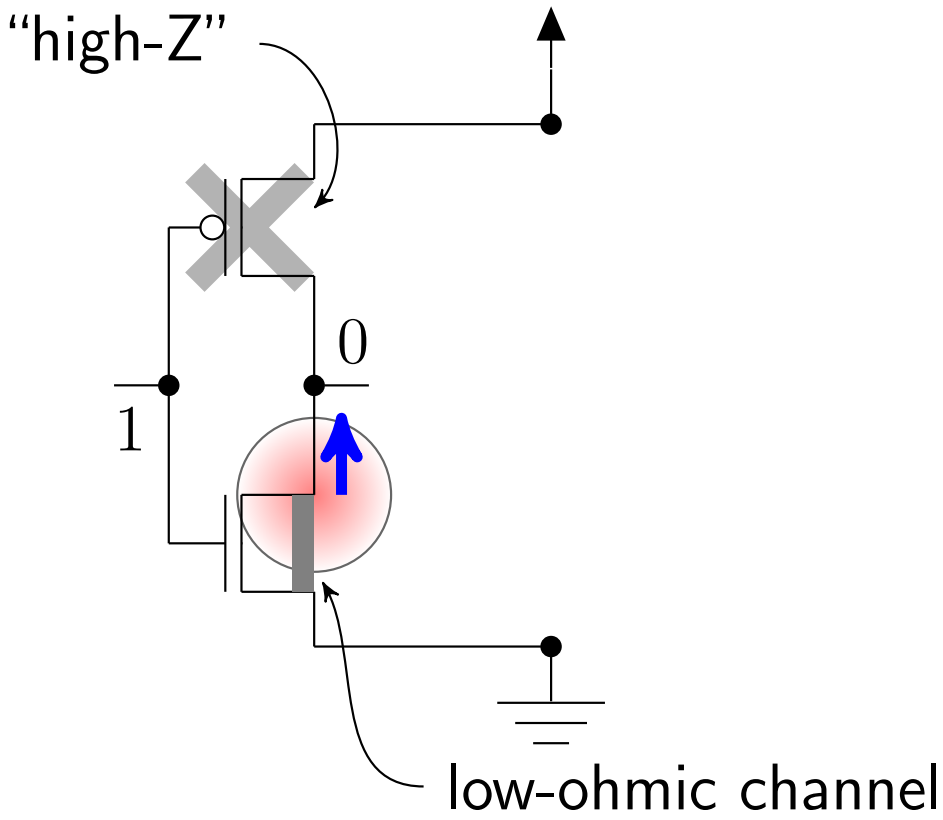
Seebeck Effect on CMOS Gates



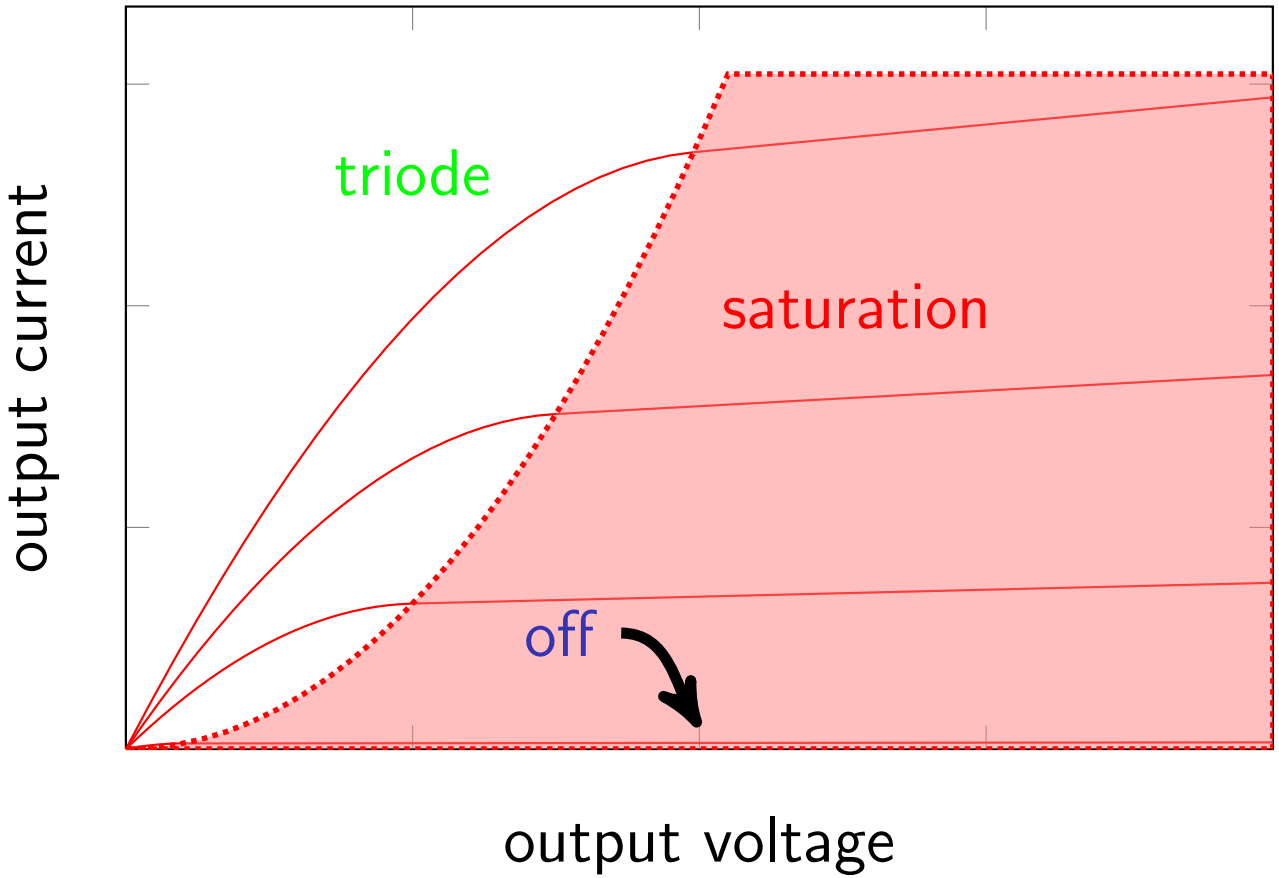
Seebeck Effect on CMOS Gates



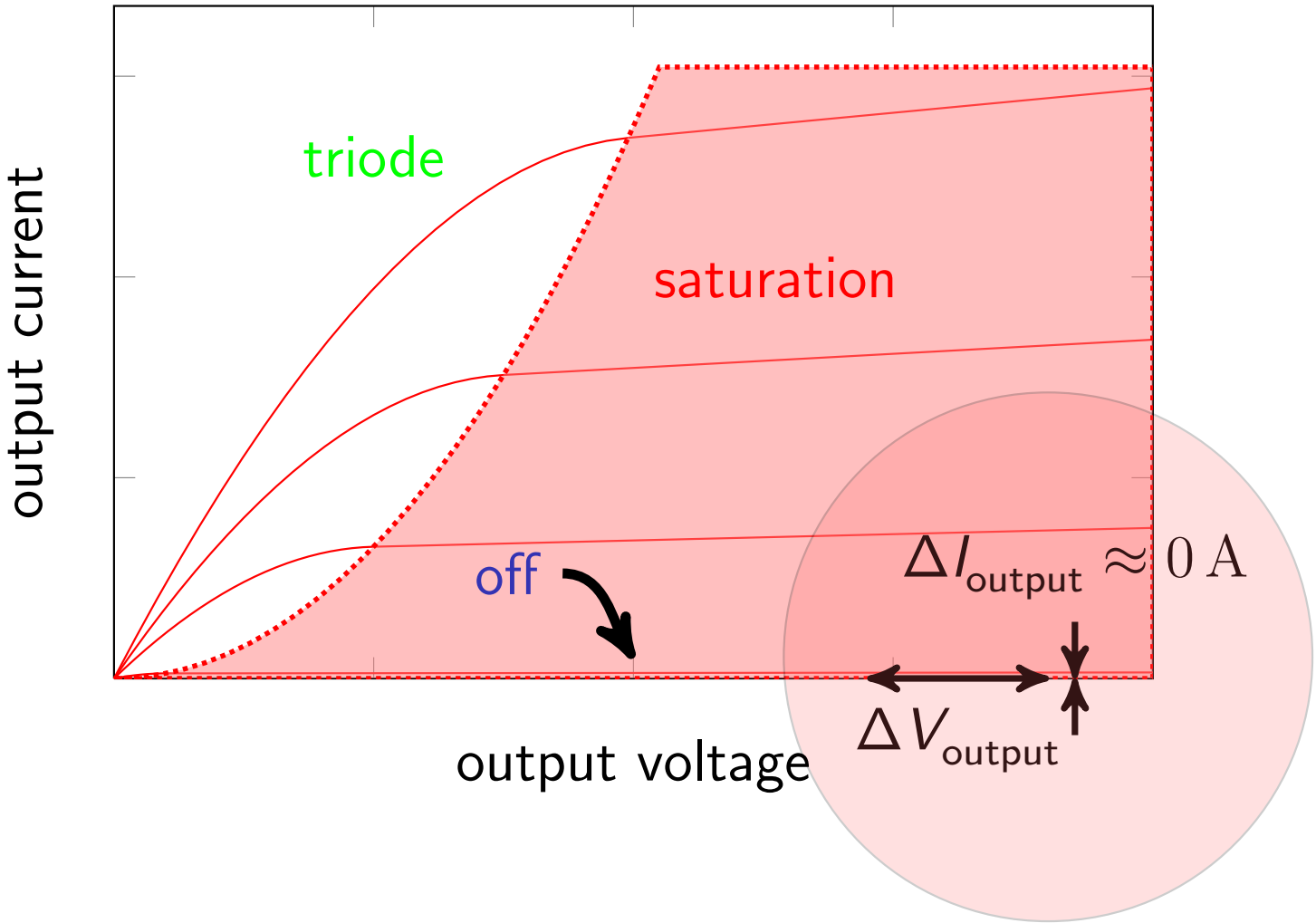
Seebeck Effect on CMOS Gates



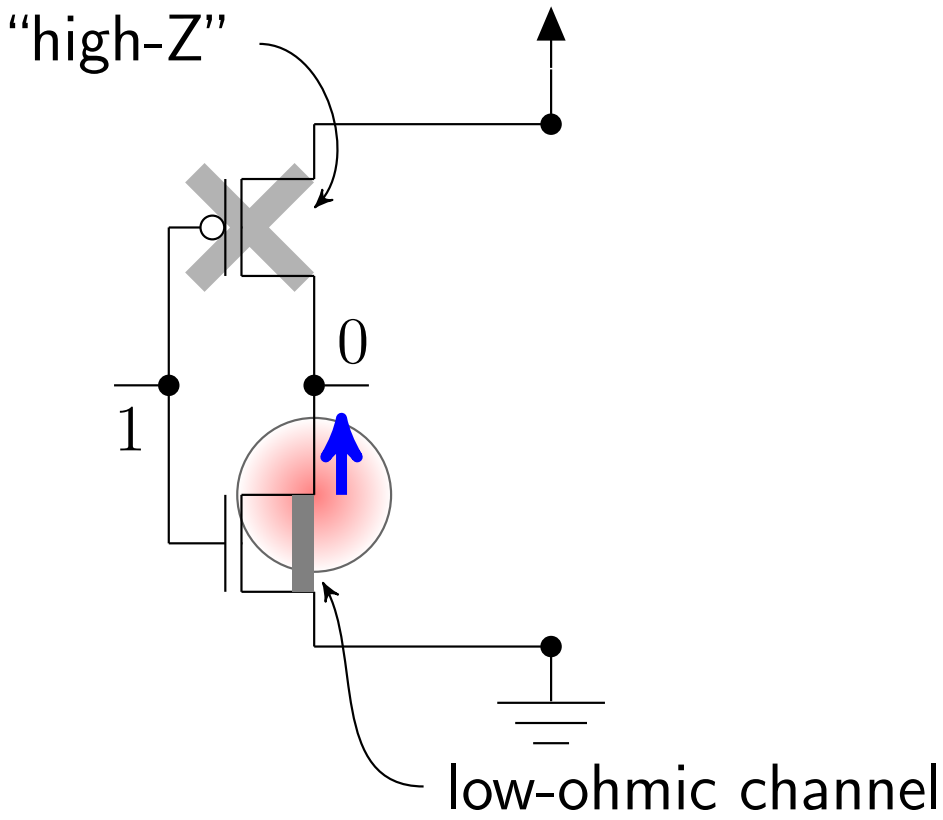
MOS Transistor Output Characteristic



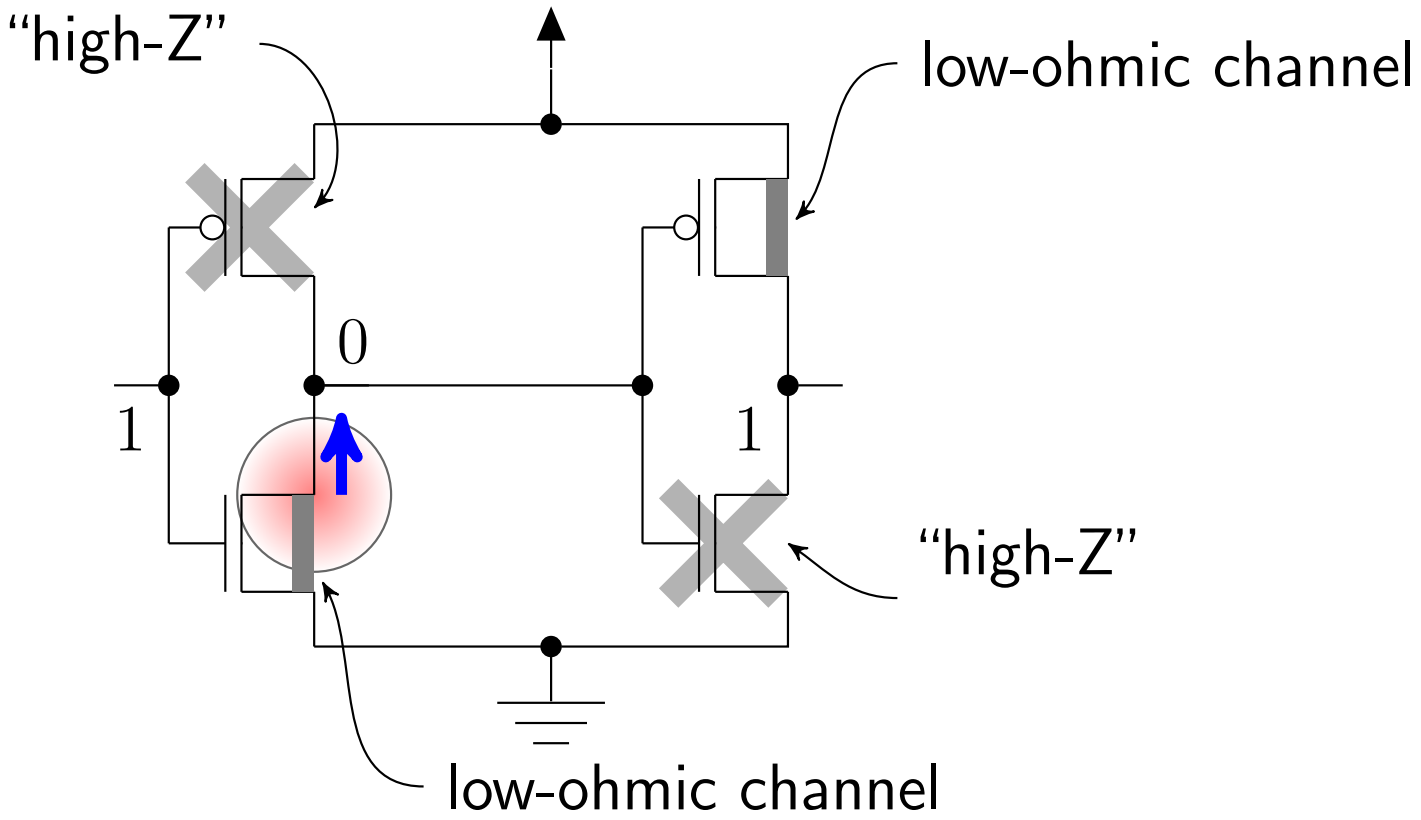
MOS Transistor Output Characteristic



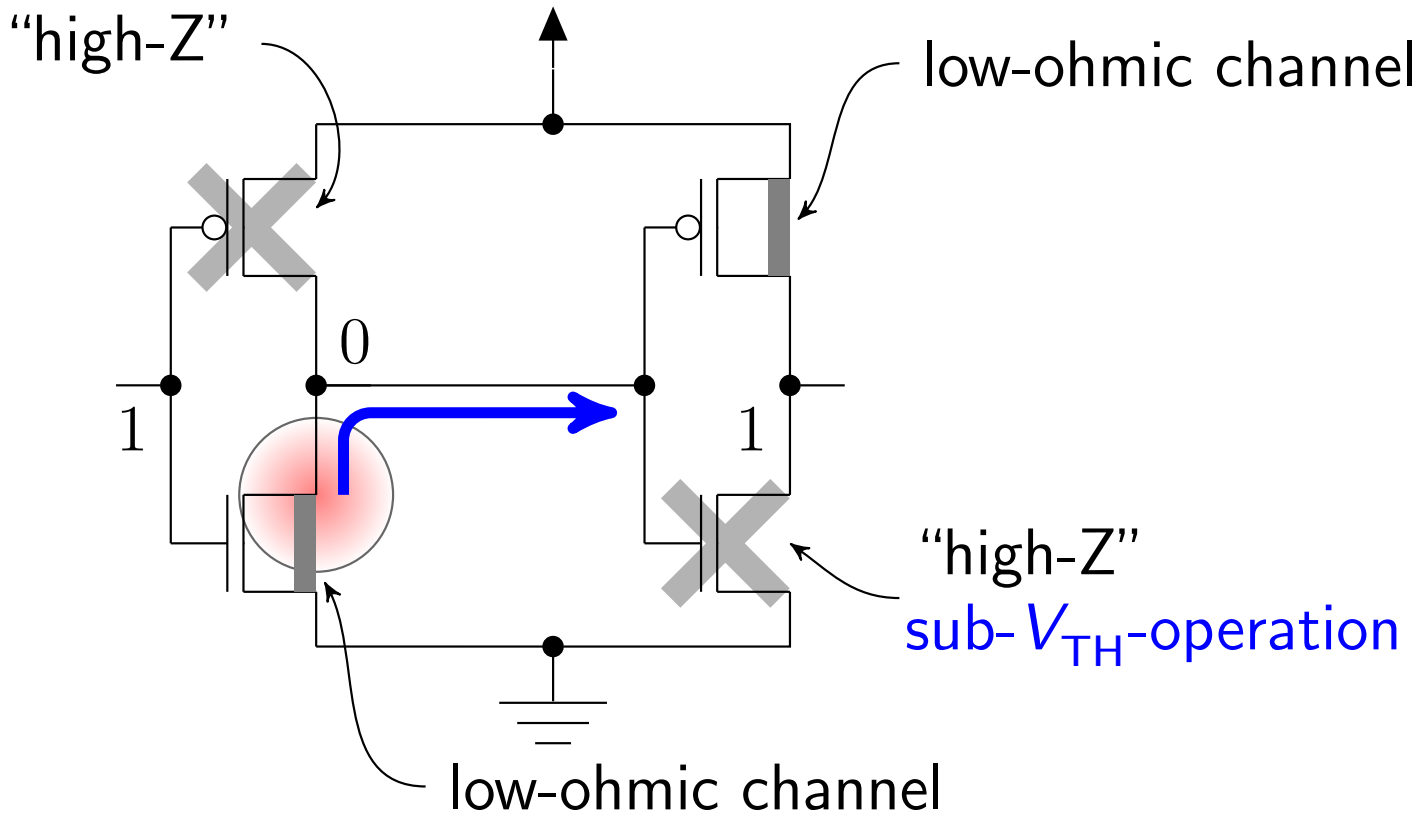
Seebeck Effect on CMOS Gates



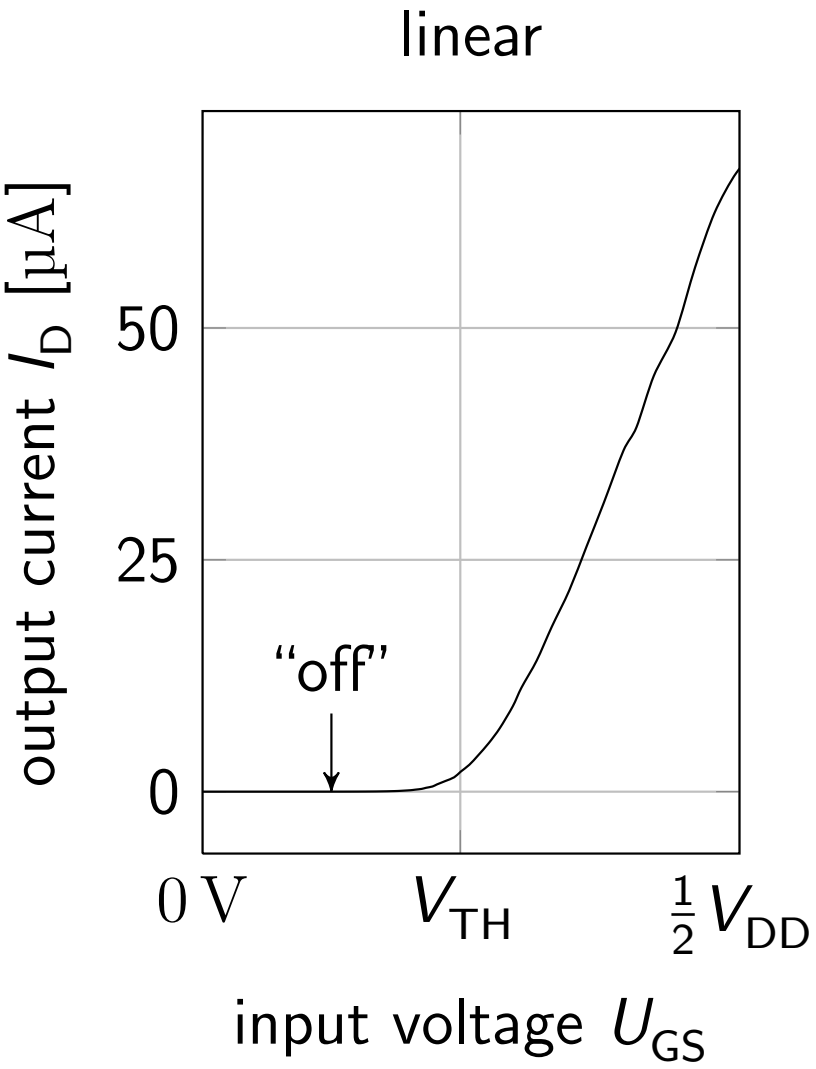
Seebeck Effect on CMOS Gates



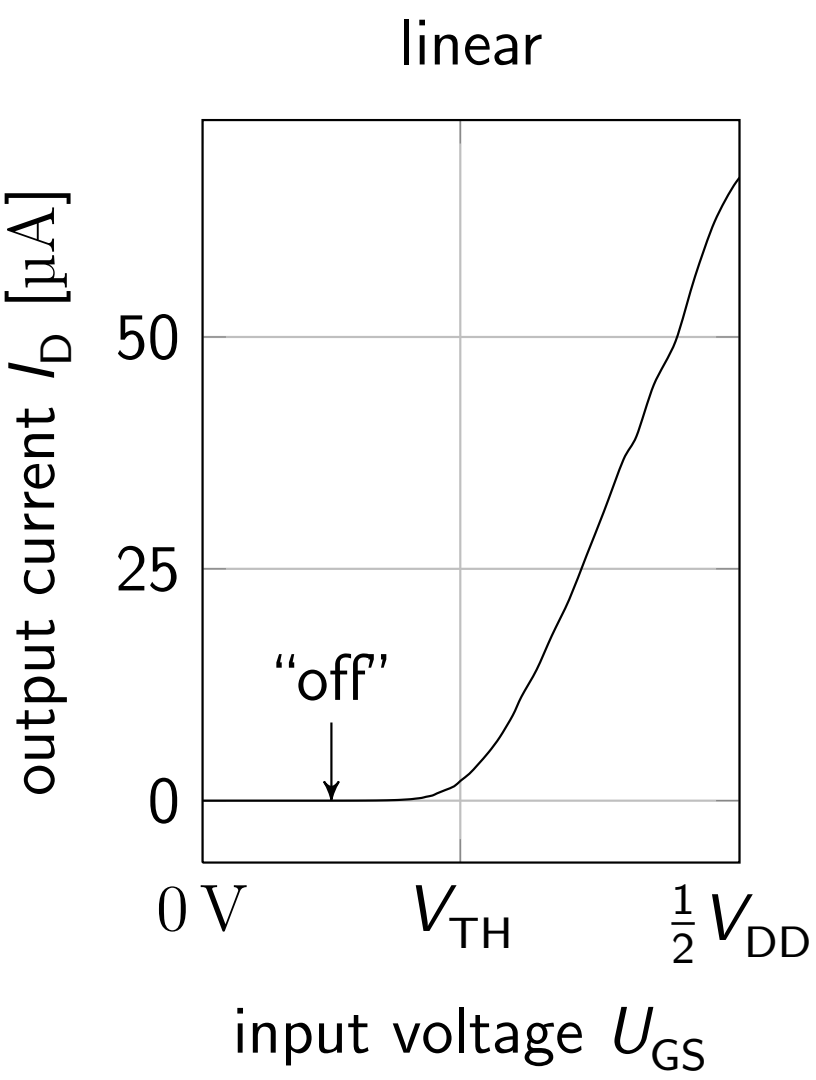
Seebeck Effect on CMOS Gates

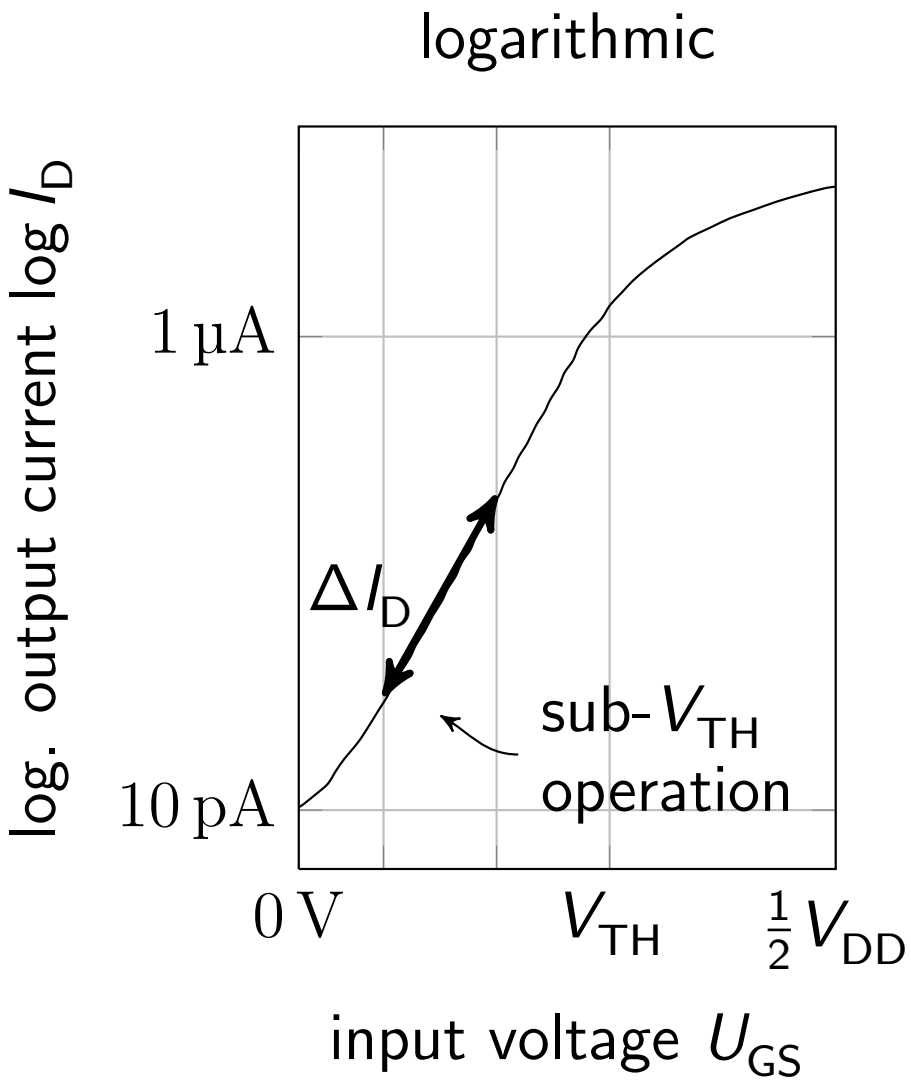


MOS Transistor Transfer Characteristic

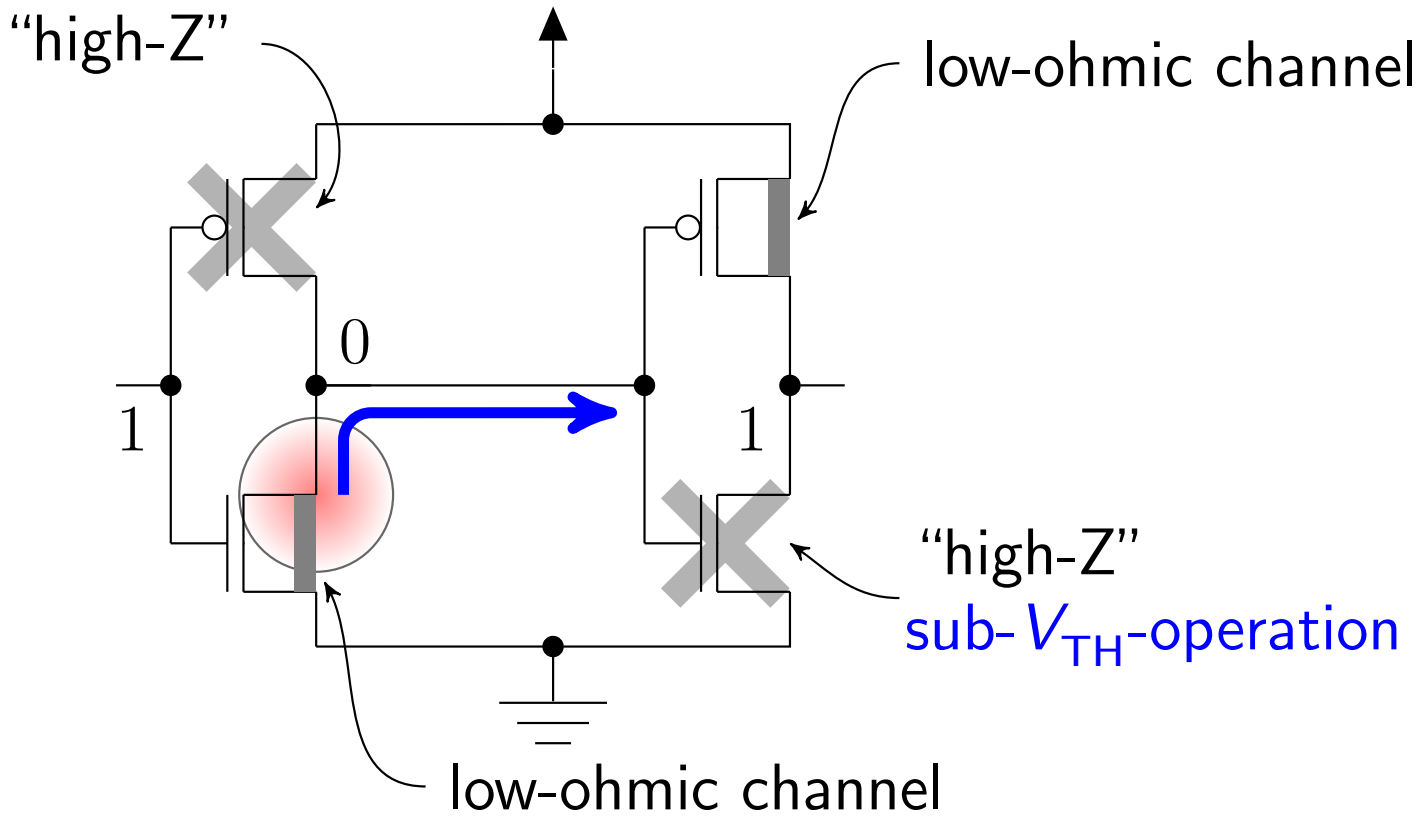


MOS Transistor Transfer Characteristic

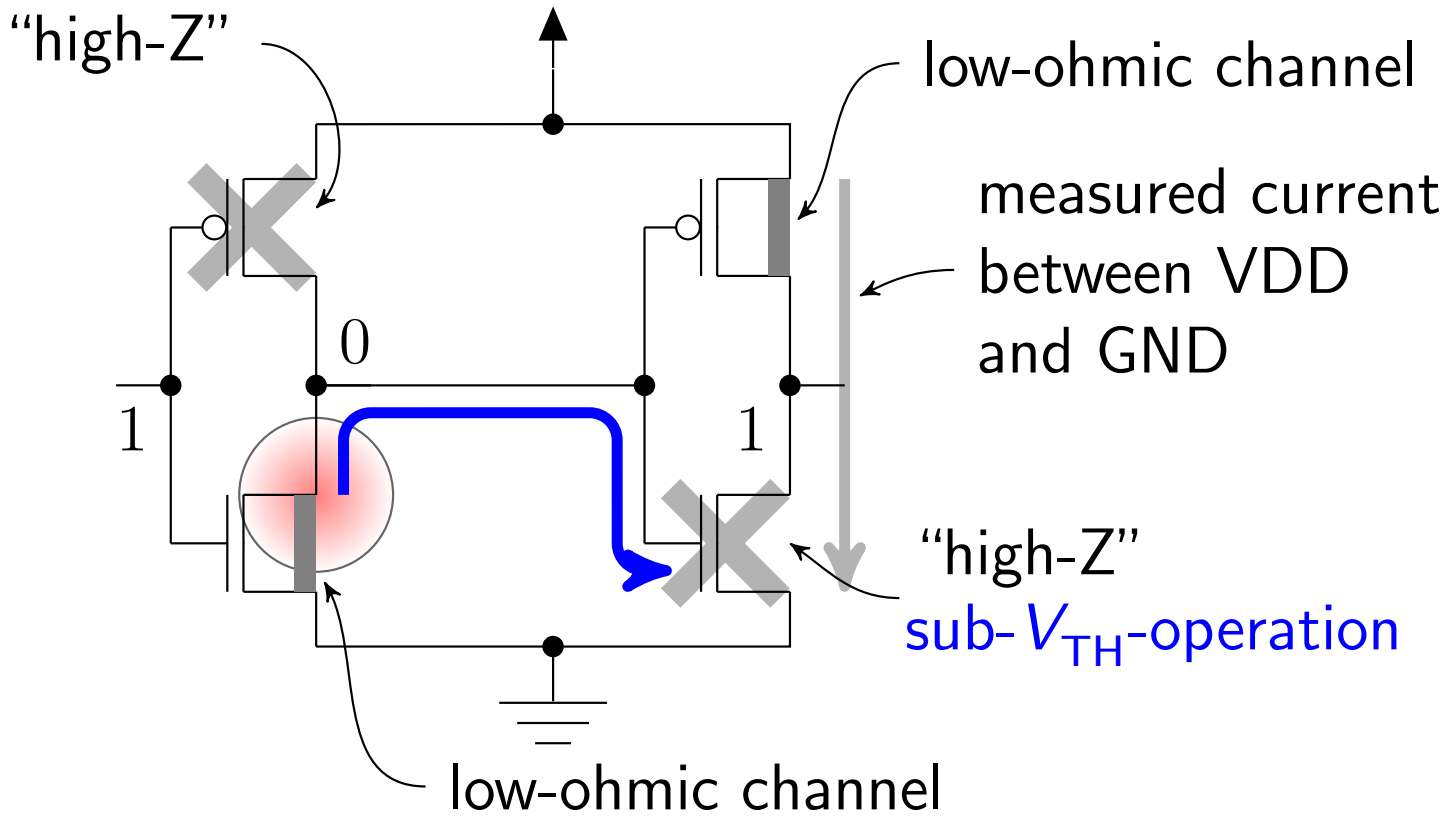




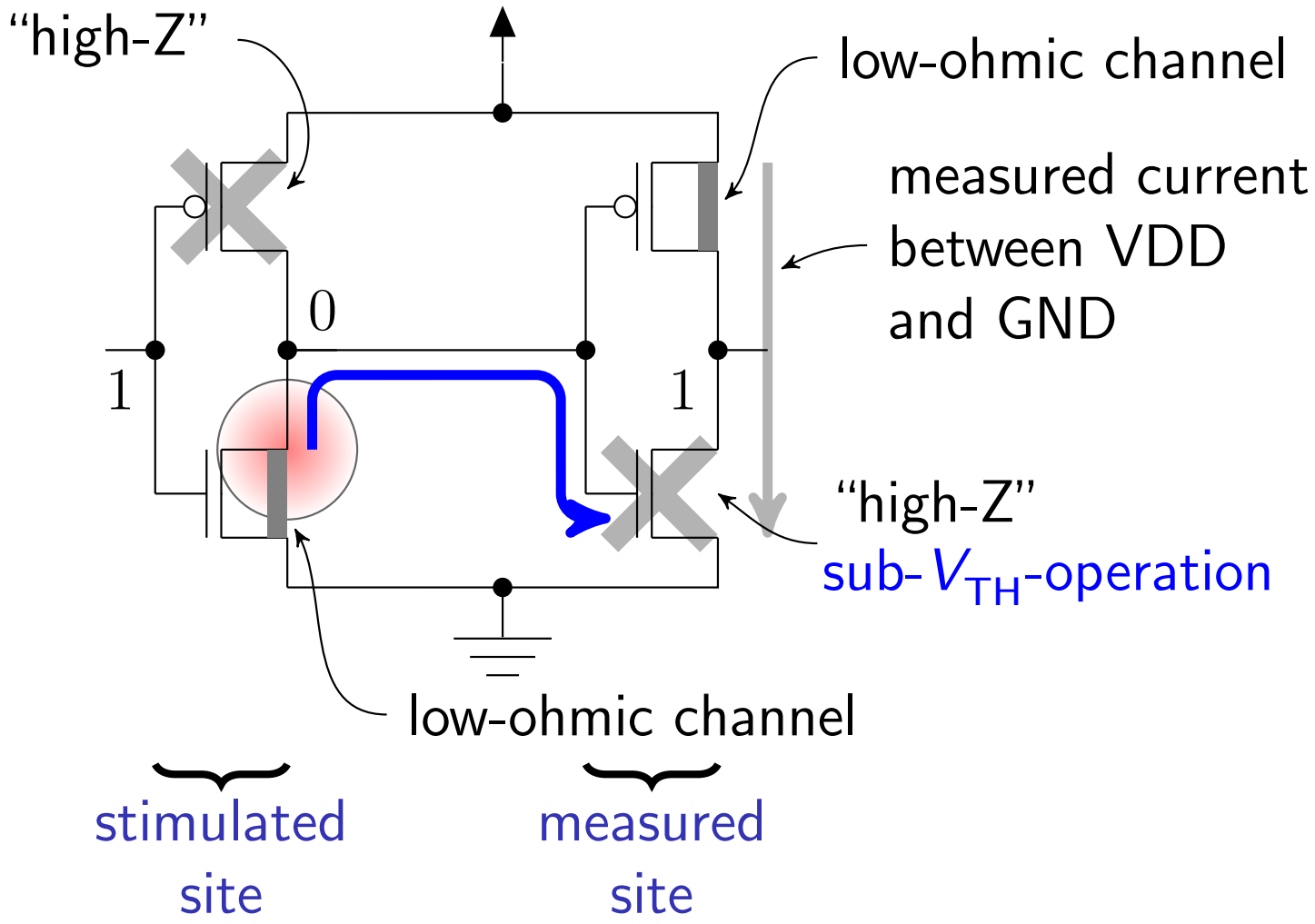
Seebeck Effect on CMOS Gates



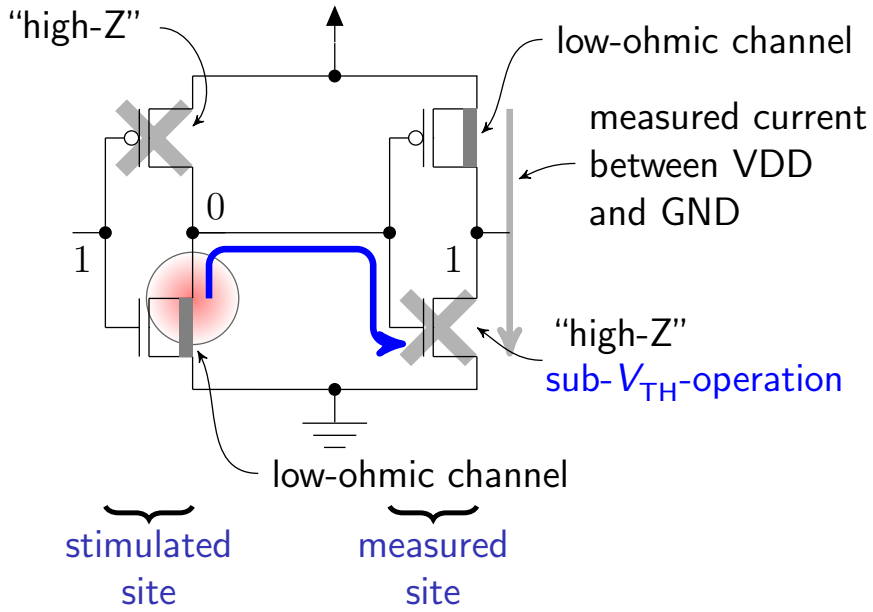
Seebeck Effect on CMOS Gates



Seebeck Effect on CMOS Gates

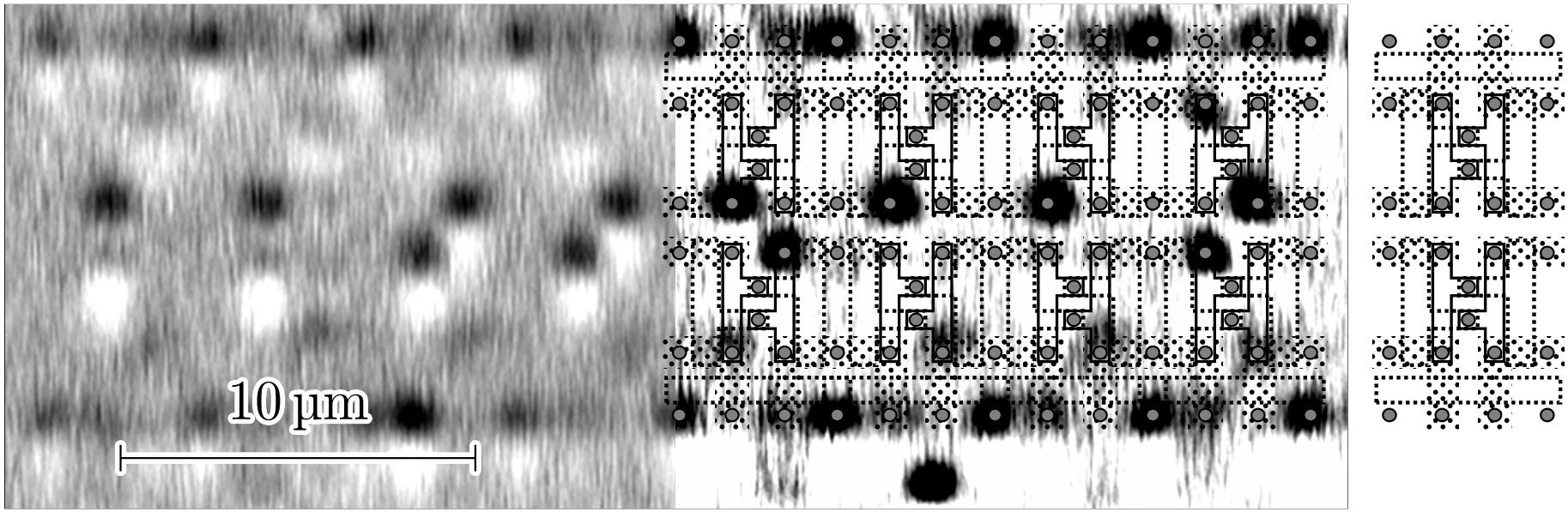


Seebeck Effect on CMOS Gates

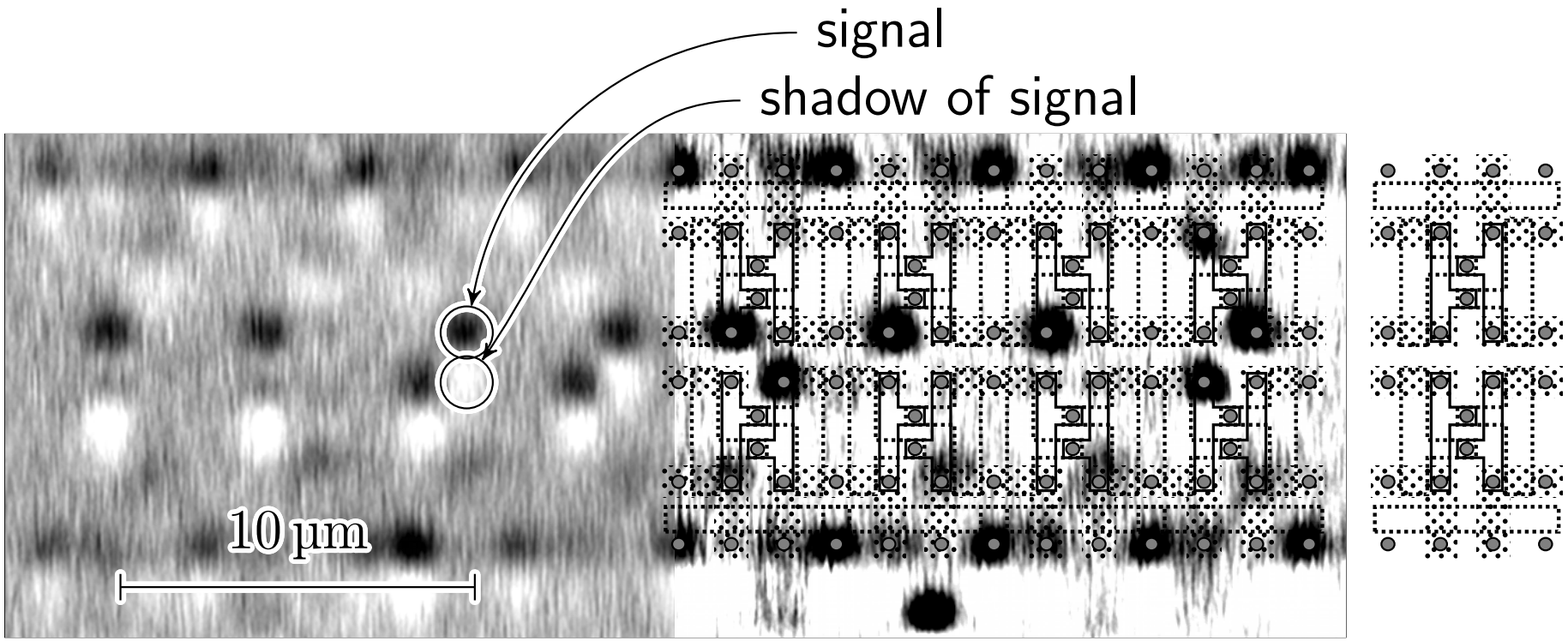


- stimulation at transistor in on state
- measurement at transistor in off state
- sub-V_{TH}-operation: very low currents need to be measured
- works with all CMOS logic gates – though more complex

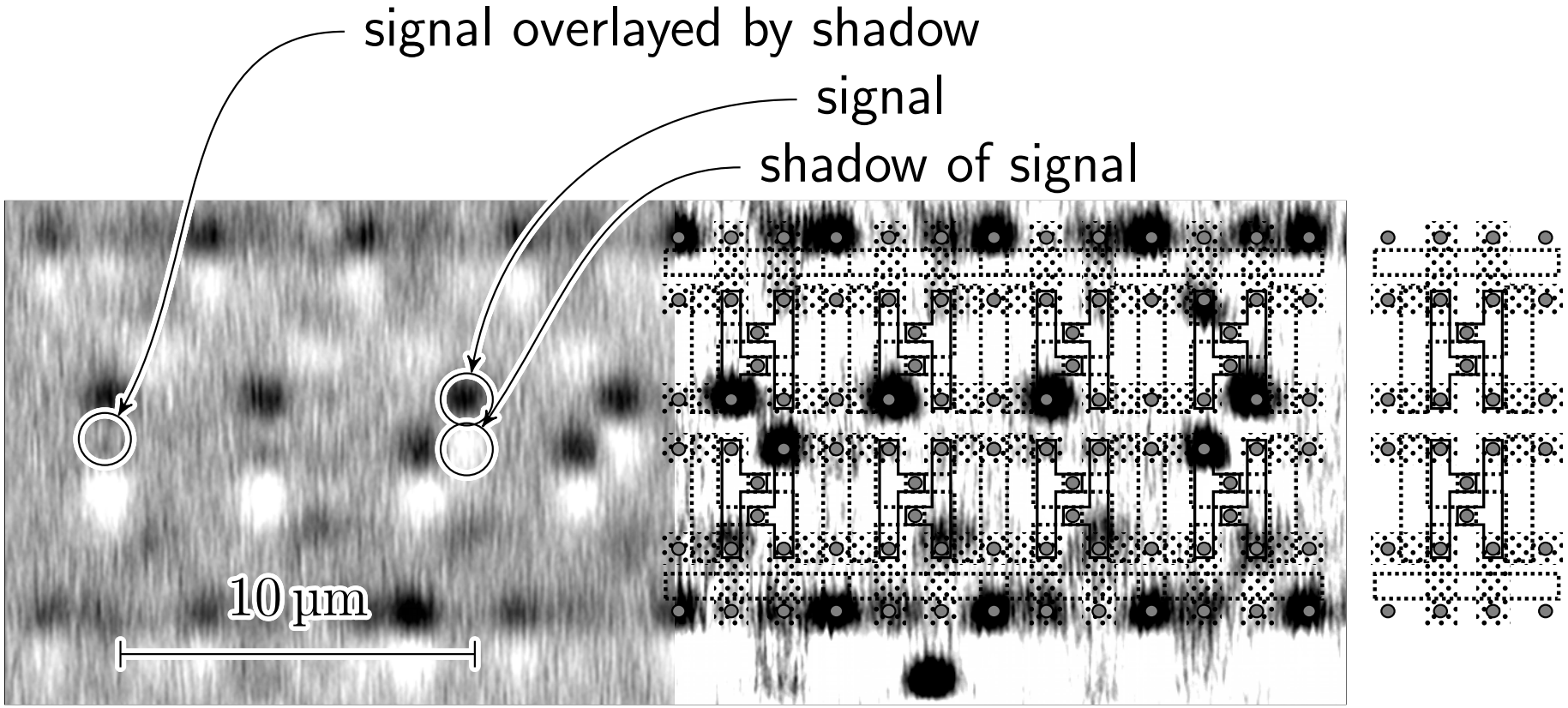
SRAM (PUF) Characterization



SRAM (PUF) Characterization



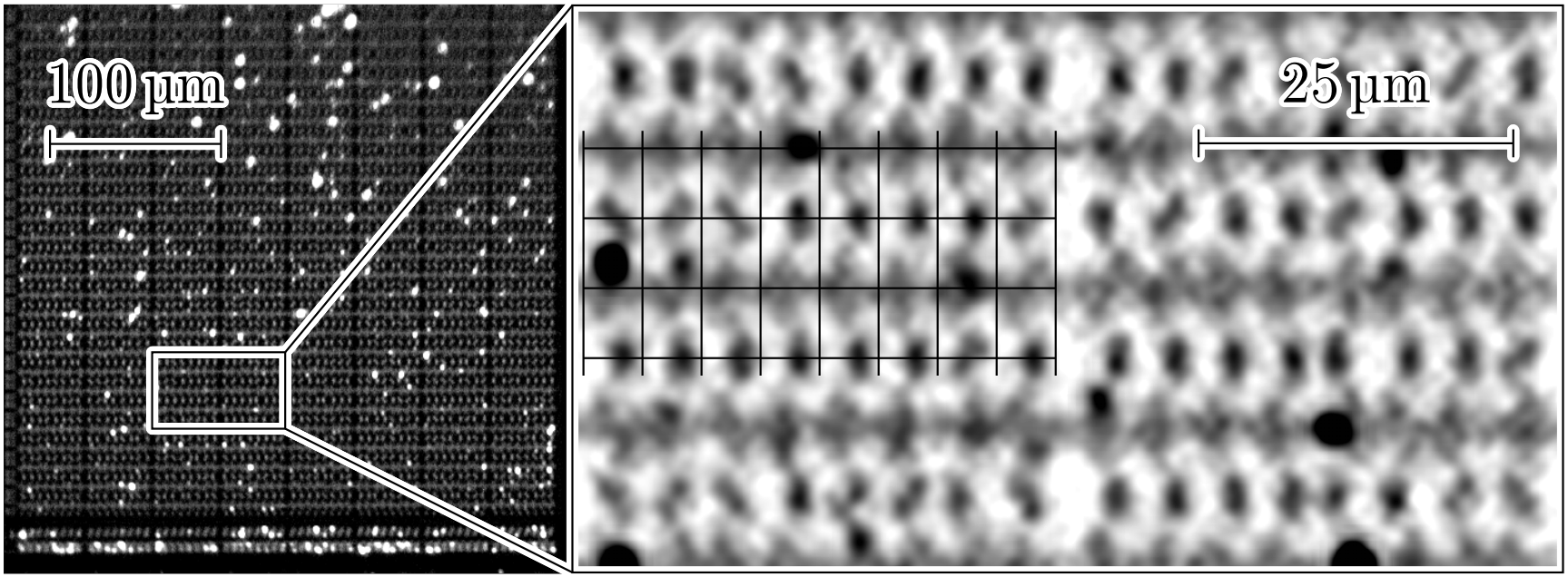
SRAM (PUF) Characterization



Increased SRAM size

full image

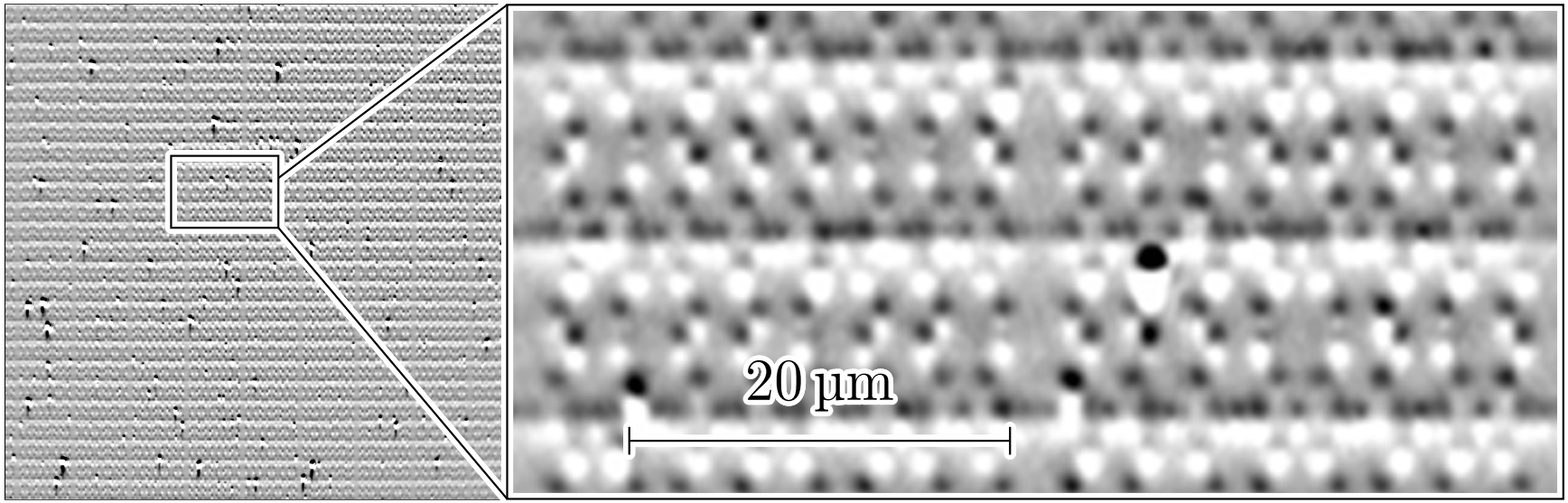
enlarged section



- ATMega328P SRAM PUF PoC implementation, $\approx 600\,\mathrm{nm}$
- $\approx 500 \times 8$ bit of SRAM, single trace

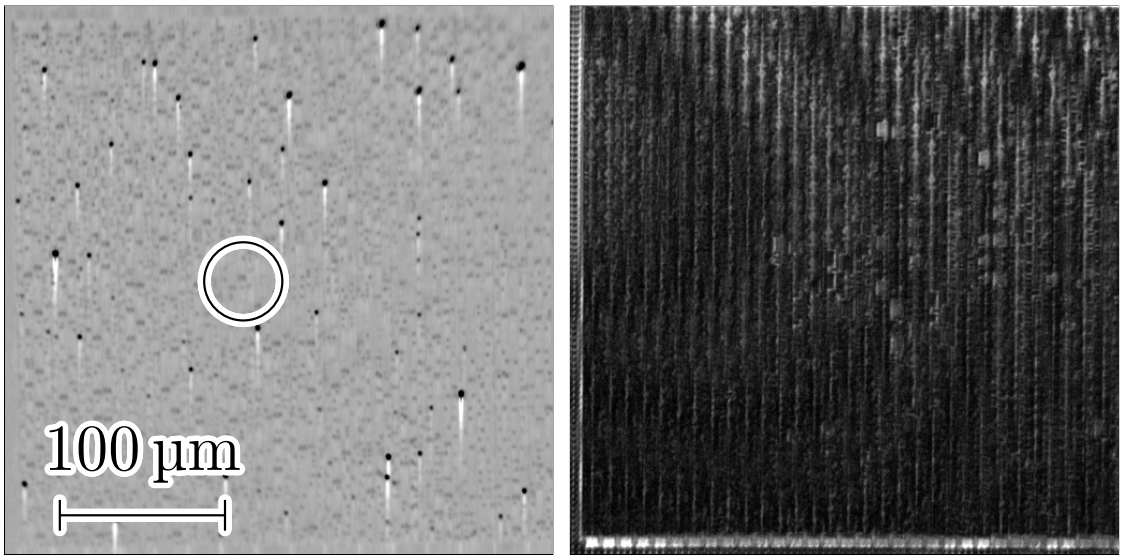
Shrinking Technology

full image enlarged section

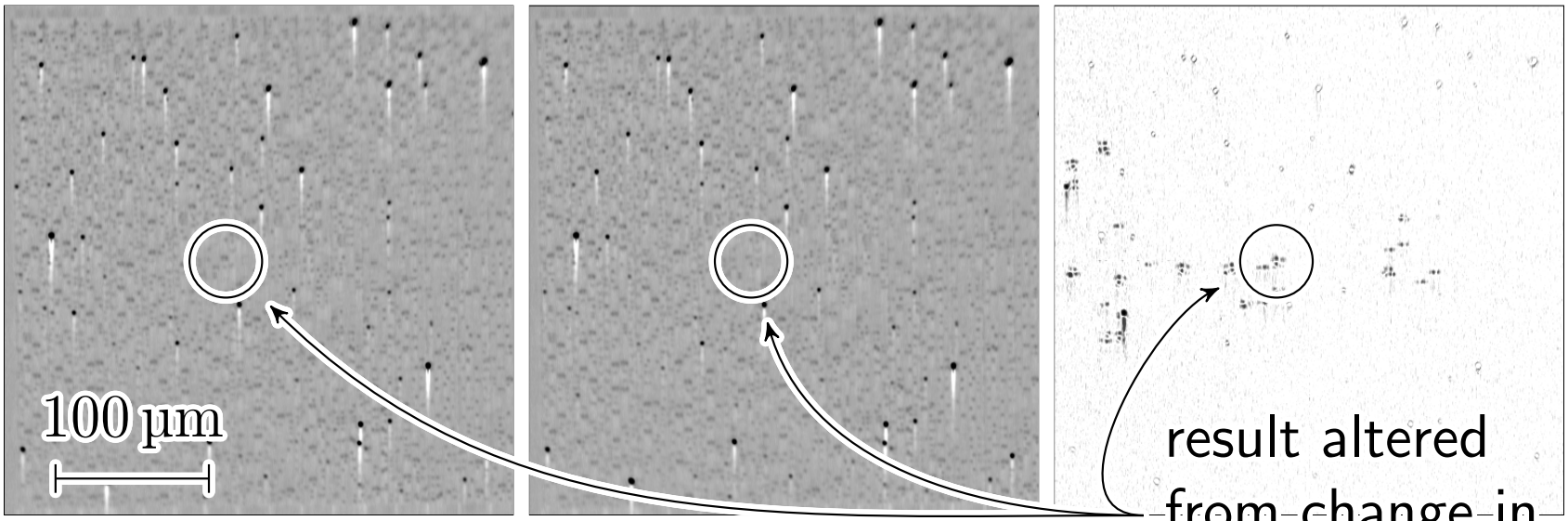


- ATXMega128A1 SRAM PUF PoC implementation, $\approx 300\,\mathrm{nm}$
- $\approx 900 \times 8$ bit of SRAM, single trace

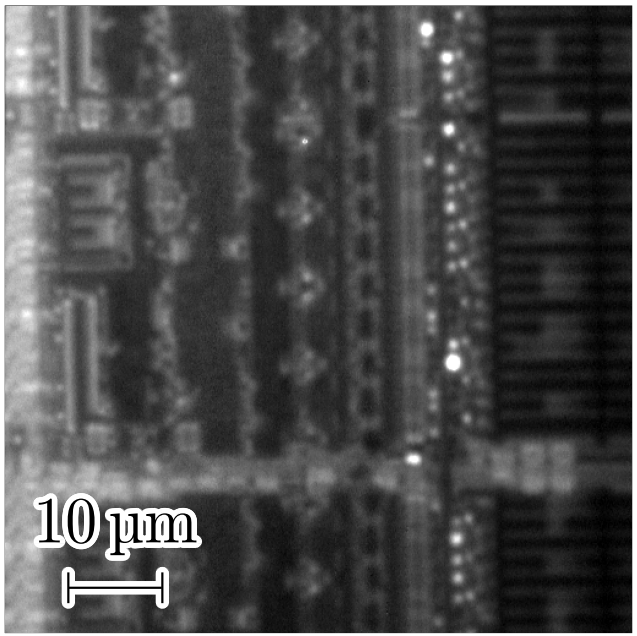
Reading Synthesized Logic



Reading Synthesized Logic



Semi-Invasive Memory Reading



- Memory Encryption Decryption (MED) unit of Infineon SLE66PE
- halted by reduced power supply ($0.7\,\mathrm{V}$)
- SRAM retains contents but reset prevents erasure

Clone SRAM – Episode II

Requirements

- circuit at least partly powered
  - connect device, be careful with light, sensors, etc.
- static, no running clock
  - clock: invasively control, reduce supply voltage, ...
  - reset: prevent data erasure, only required for registers
- low and constant current consumption
  - destructively disconnect loads, reduce supply voltage, ...

Benefits

- extract logic state of SRAM and register in single trace
- scalable to huge areas

Clone SRAM – Episode II

- SRAM
  - we know whats in there
  - PUF: very easy characterization
- Register
  - we can find out what's in there
  - PUF: well . . . just as SRAM
  - as part of other type of PUF: better but still vulnerable
- PUFs are only part of the system

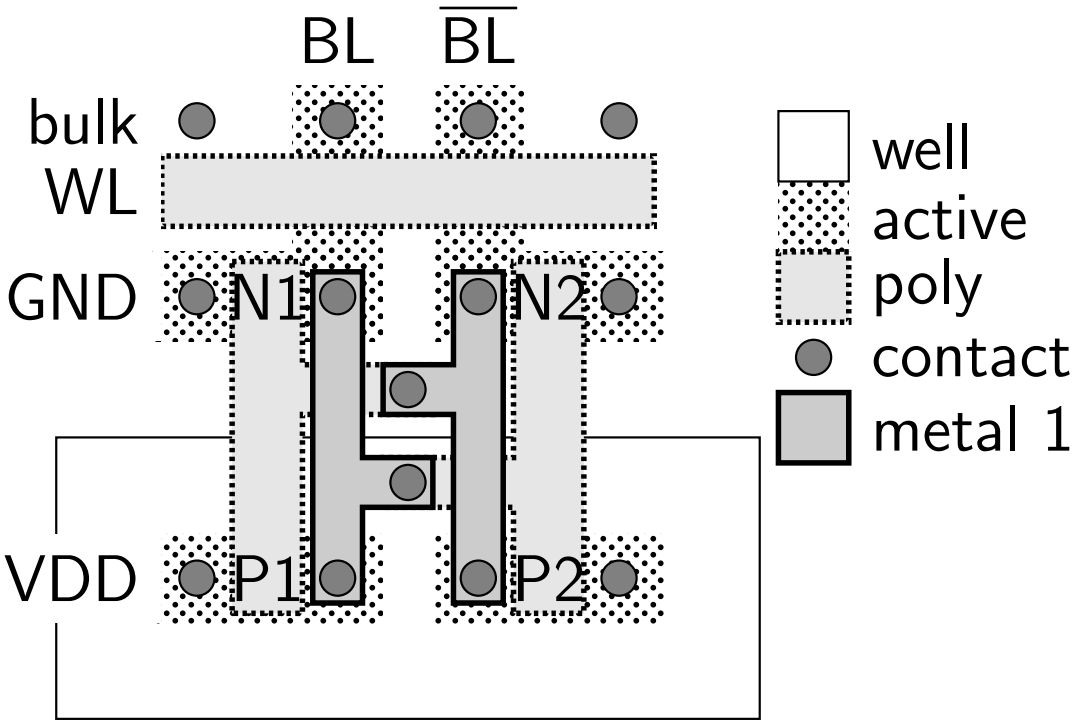
Thank you for your attention!

This work has been supported by:

Helmholtz Research School on Security Technologies

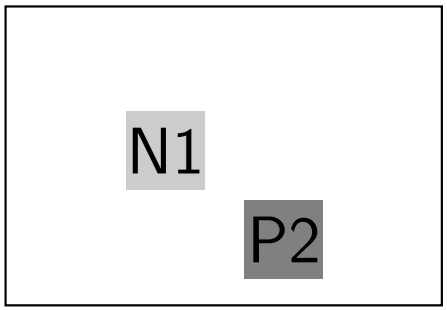
picture by Arne Hückelheim

6T-Cell SRAM Layout



Possible Responses:

0:



1: