An Alternative to Error Correction for SRAM-Like PUFs

Maximilian Hofer & Christoph Böhm
Graz University of Technology, Austria
Institute of Electronics

Project Information

Physically Uncloneable Keymaterial Extraction on Silicon (PUCKMAES)

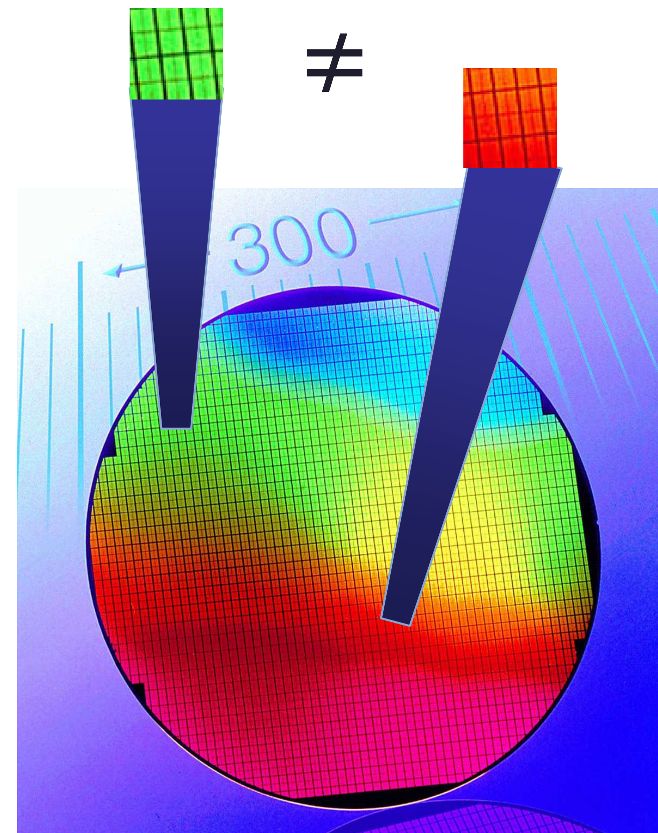
Österreichische Forschungsförderungsgesellschaft FFG (FIT-IT) funded

Partners:

- University of Technology Graz, Institute of Electronics
- Infineon Austria AG

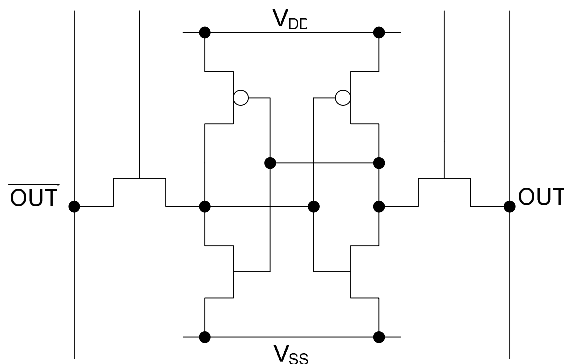
What are Physical Unclonable Functions?

- Read out fingerprint-like data of device controlled by certain function.
- Data is based on process variations.
- Example: Threshold voltage of transistors (doping concentration).
- Usage: Identification, Key-Generation for crypt. purposes.



SRAM-PUFs

SRAM-Cell:

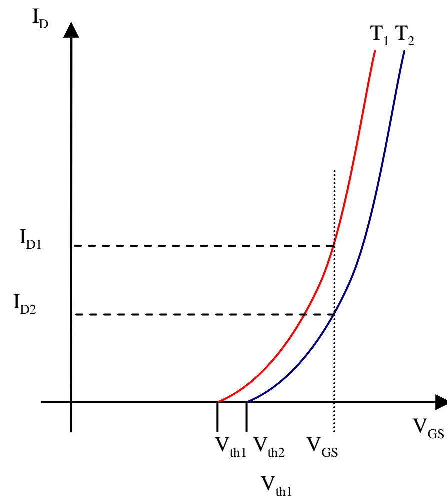


Usage:

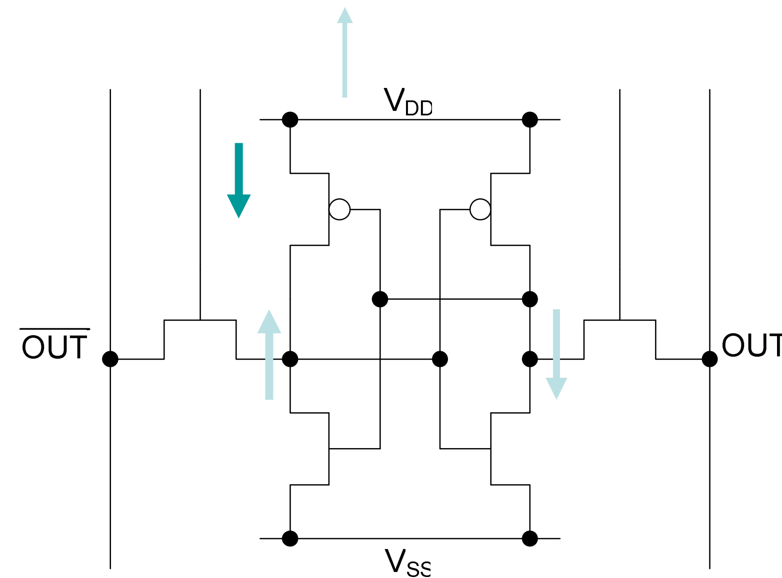
- Initial condition: All nodes are at VSS.
- SRAM-cell is powered-up.
- Due to mismatch between nominal identical transistors the cell provides same output at OUT (HIGH/LOW) after every power-up procedure.

Introduction to SRAM-PUFs

Mismatch between two transistors:



Power-up SRAM-cell:



Problem

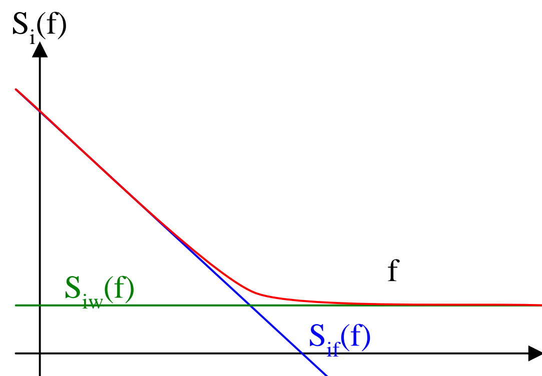
SRAM-like physical unclonable functions (PUFs) exhibit error-rate of 10% due to random and deterministic errors.

Ways to handle high error-rates:

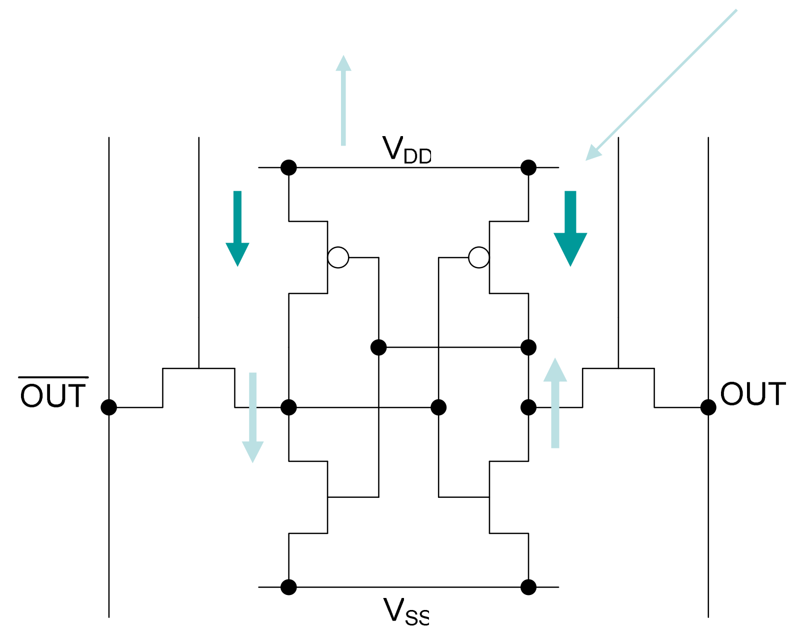
- Find adequate error correction approach.
- Improve cell design.
- Chose those cells that provide stable behavior.

Random Errors

Noise (Error rate: → 0.5%)

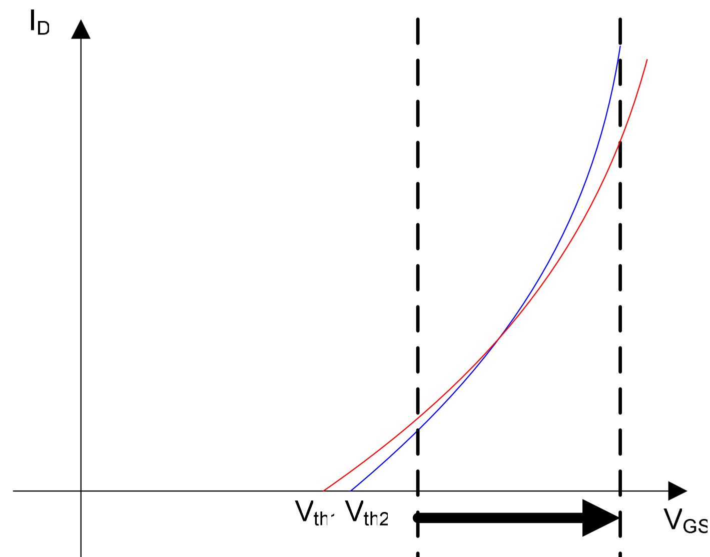


Flicker (1/f) and thermal noise



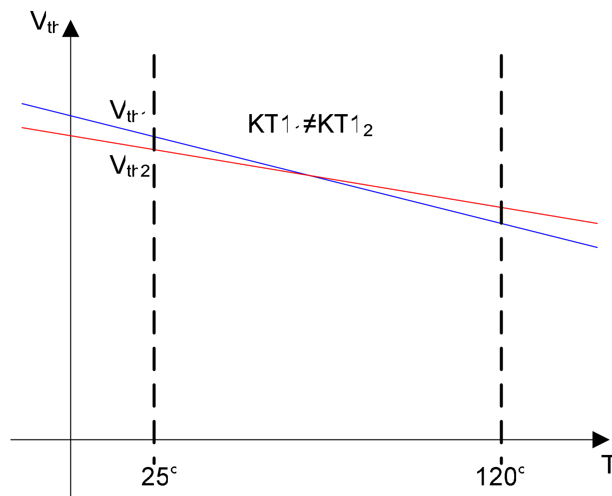
Deterministic Errors

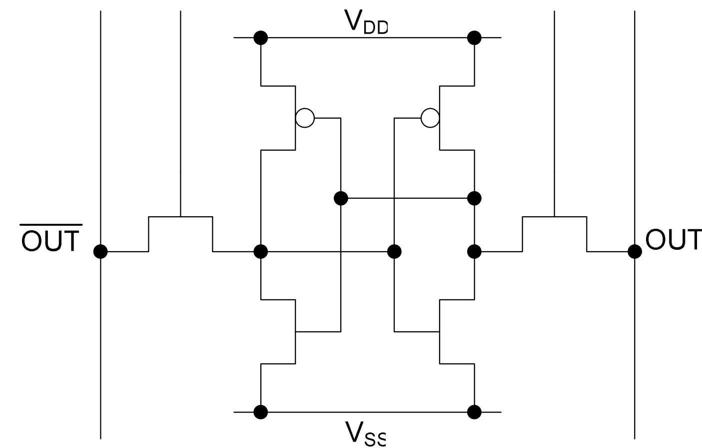
VDD (Error rate: 0.5% → 2%)



Deterministic Errors

Temperature (Error rate: 0.5 → 6%)

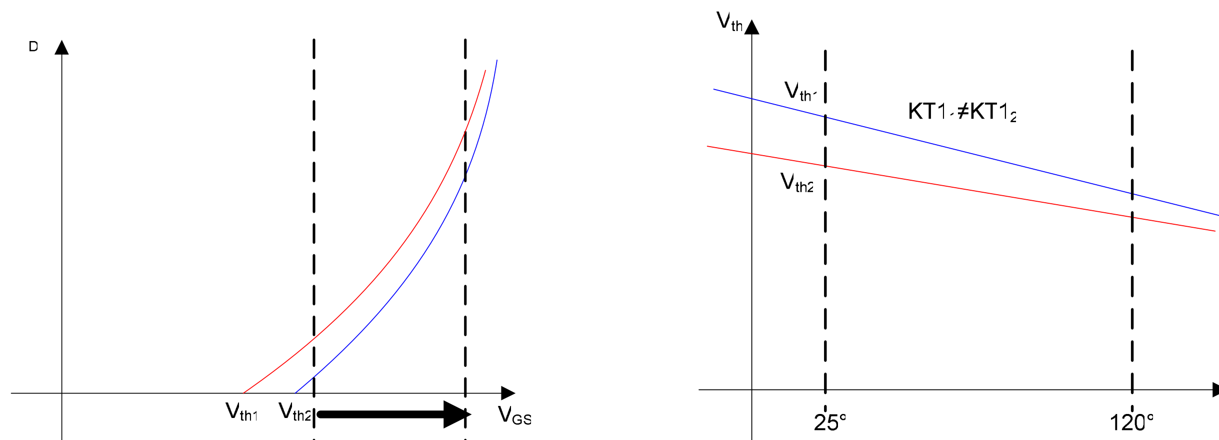




PUF-Cell Selection

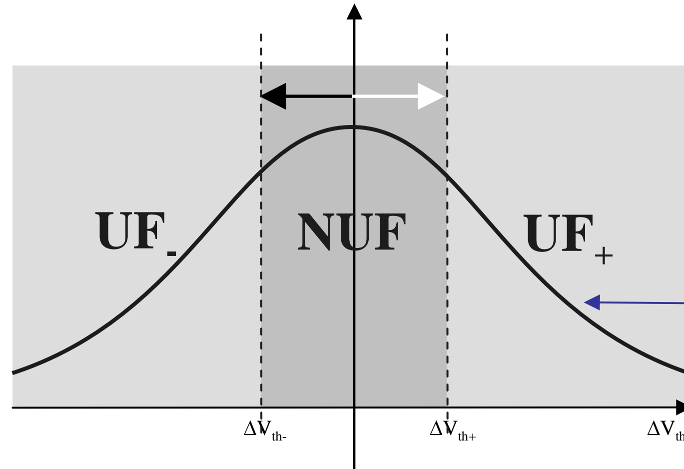
Approach: Select those cells that provide a reasonable degree of mismatch:

- Influence of noise becomes smaller.
- No output-hopping within region of operation.



Define ΔVth-Threshold

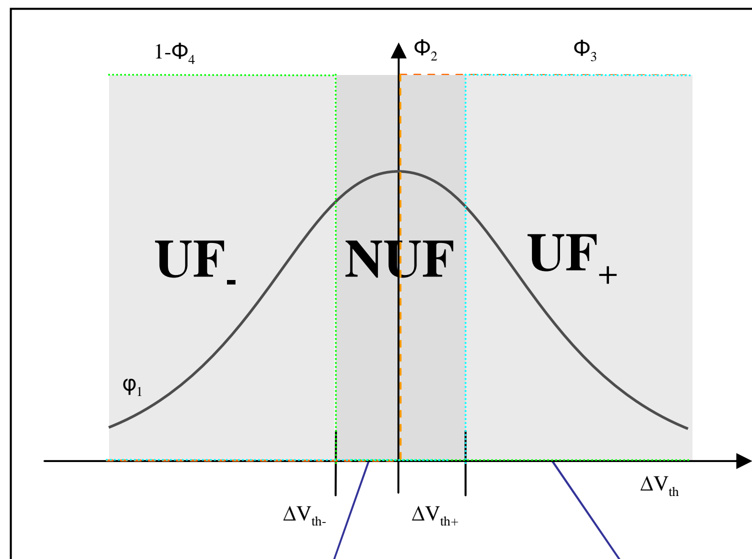
- ΔVth- and ΔVth+ define a Vth mismatch threshold.
- If the mismatch of the transistor pair exceeds that value, the PUF-cell is selected.



Distribution of Vth mismatch

Mean = zero (may not be the case if design/layout is not chosen symmetrically or if gradient on wafer exists)

Cell Output and Selection



Cell Selection

CDF of decision (no disturbance)

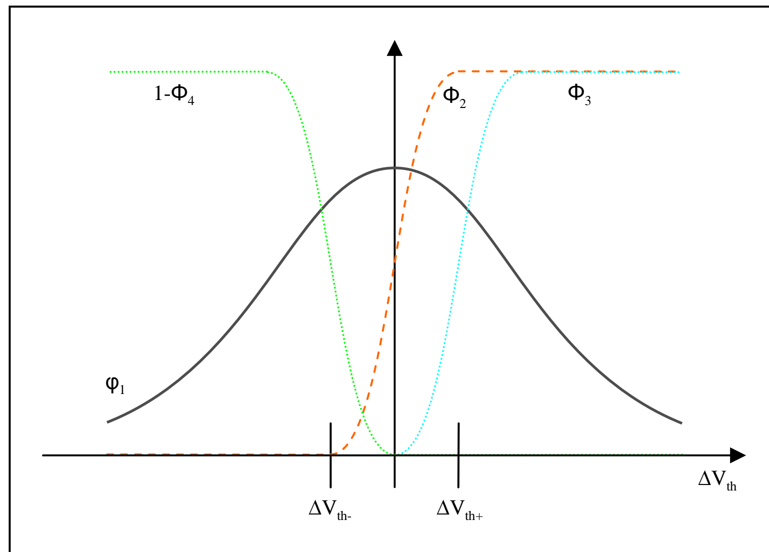
probability density function (pdf):

$$f(x) = \varphi_{\mu,\sigma}(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$$

cumulative distribution function (cdf):

$$F(x) = \Phi_{\mu,\sigma}(x) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} dx$$

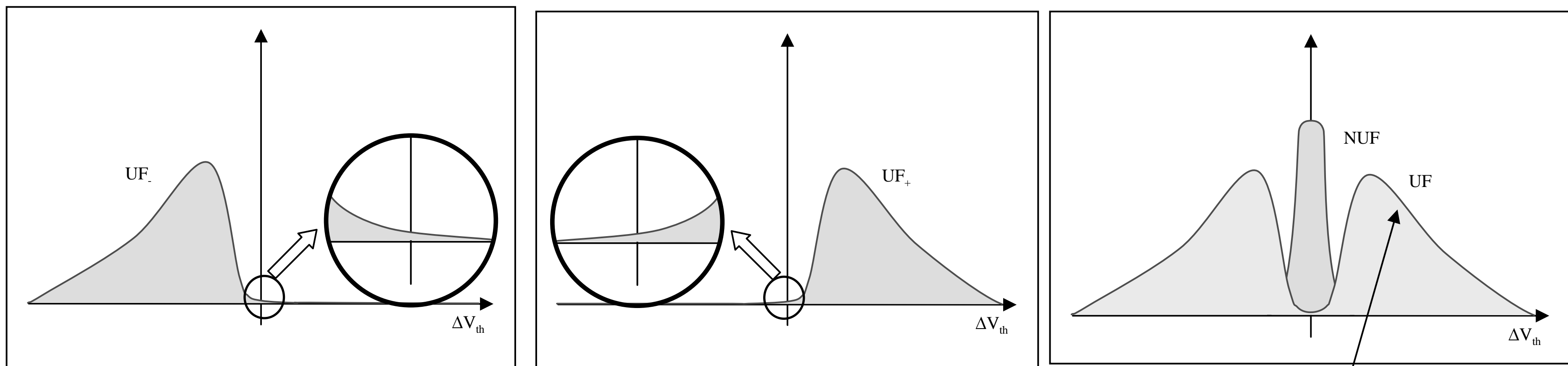
Cell Output and Selection



- Disturbances on Circuit leads to non-ideal behavior.
- Cells may not provide expected result.
- Cells are selected that do not provide sufficient mismatch.

Selecting Cells

Multiplying mismatch distribution and selection-CDF leads to the following distributions of selected cells:



Probability of occurrence of useful PUF_cells depending on ΔVth:

$$UF = \varphi_1\left[\Phi_3 + (1 - \Phi_4) - 2\Phi_3(1 - \Phi_4)\right] = \varphi_1\left[1 - \Phi_4 - \Phi_3 + 2\Phi_3\Phi_4\right]$$

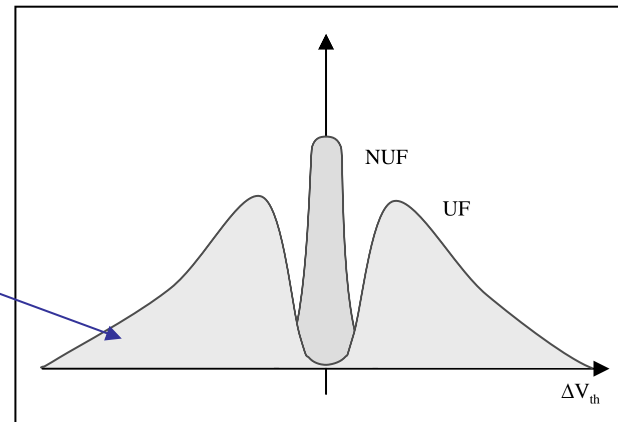
Determine Number of selected PUF-cells α

$$UF = \varphi_1 \left[\Phi_3 + (1 - \Phi_4) - 2\Phi_3 (1 - \Phi_4) \right] = \varphi_1 \left[1 - \Phi_4 - \Phi_3 + 2\Phi_3 \Phi_4 \right]$$

$$\alpha = \int_{-\infty}^{+\infty} UF dV_{th}$$

$$\alpha = 1 - \frac{1}{\sigma_1 2\pi} \int_{-\infty}^{+\infty} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_1}{\sigma_1}\right)^2} \left[\frac{1}{\sigma_4} \int_{-\infty}^{x} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_4}{\sigma_4}\right)^2} dV_{th} + \frac{1}{\sigma_3} \int_{-\infty}^{x} e^{-\frac{1}{2}\left(\frac{V_{th}-\mu_3}{\sigma_3}\right)^2} dV_{th} - \frac{2}{\sigma_3 \sigma_4 \sqrt{2\pi}} \int_{-\infty}^{dV_{th}} e^{-\frac{1}{2}\left(\frac{dV_{th}-\mu_3}{\sigma_3}\right)^2} dV_{th} \int_{-\infty}^{dV_{th}} e^{-\frac{1}{2}\left(\frac{dV_{th}-\mu_4}{\sigma_4}\right)^2} dV_{th} \right] dV_{th}$$

Determine area under UF



Determine Error-Rate *e*

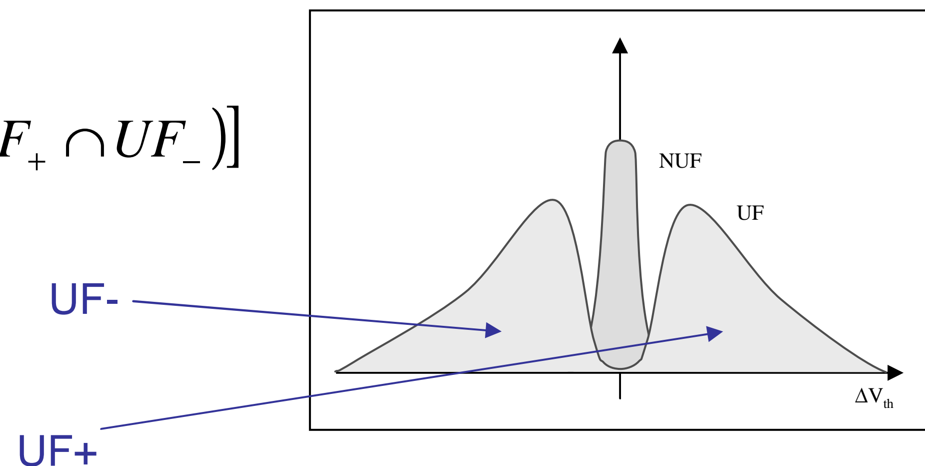
$$e = \int_{-\infty}^{+\infty} e(\Delta V_{th})\ d\Delta V_{th}$$

$$e(\Delta V_{th}) = e_+(\Delta V_{th}) + e_-(\Delta V_{th})$$

$$e_-(\Delta V_{th}) = \frac{1}{\alpha}\Phi_2\left[UF_- - \left(UF_+ \cap UF_-\right)\right]$$

$$e_+(\Delta V_{th}) = \frac{1}{\alpha}\left(1-\Phi_2\right)\left[UF_+ - \left(UF_+ \cap UF_-\right)\right]$$

Total error at certain ΔVth is sum of errors coming from UF- and UF+



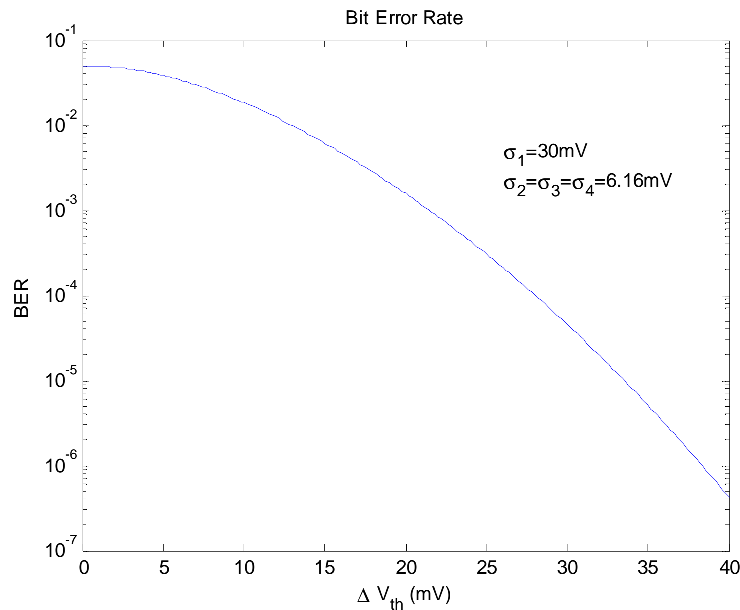
UF-

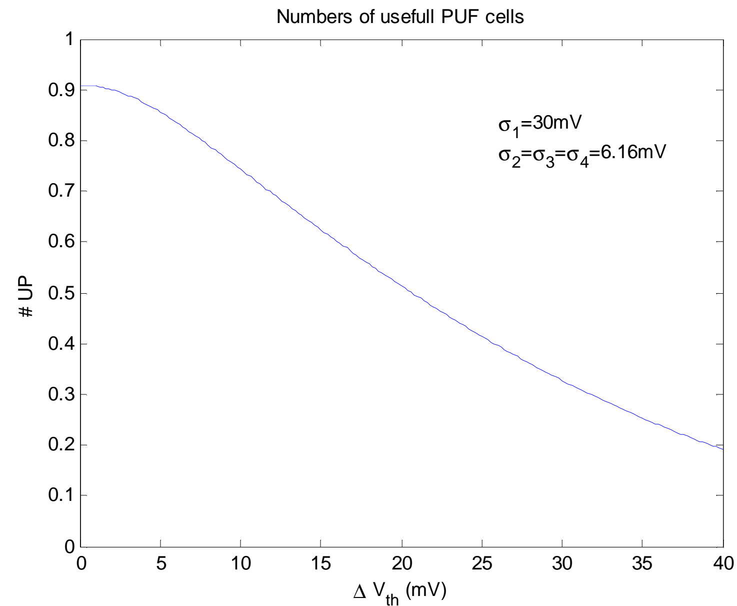
UF+

Example

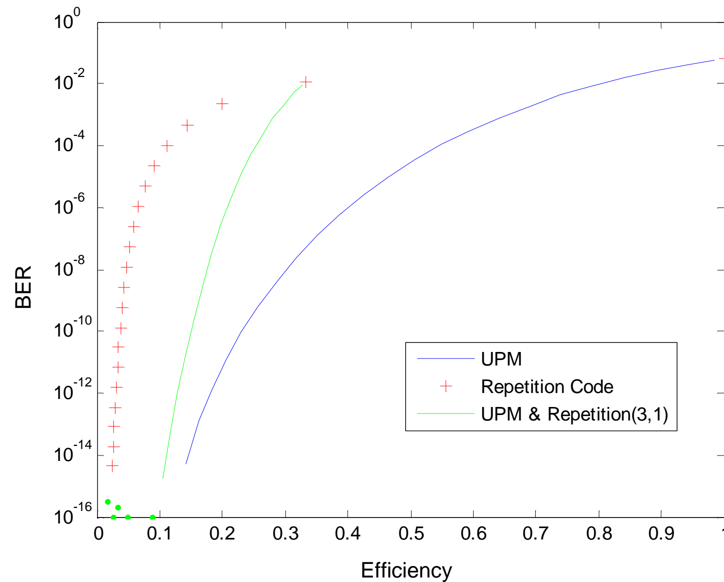
Standard Deviation σ_1 of ΔVth: 30mV

Error-Rate: 5% → $\sigma_{2,3,4}$= 6.16mV





Pre-Selection vs. Repetition Code



Scenario:

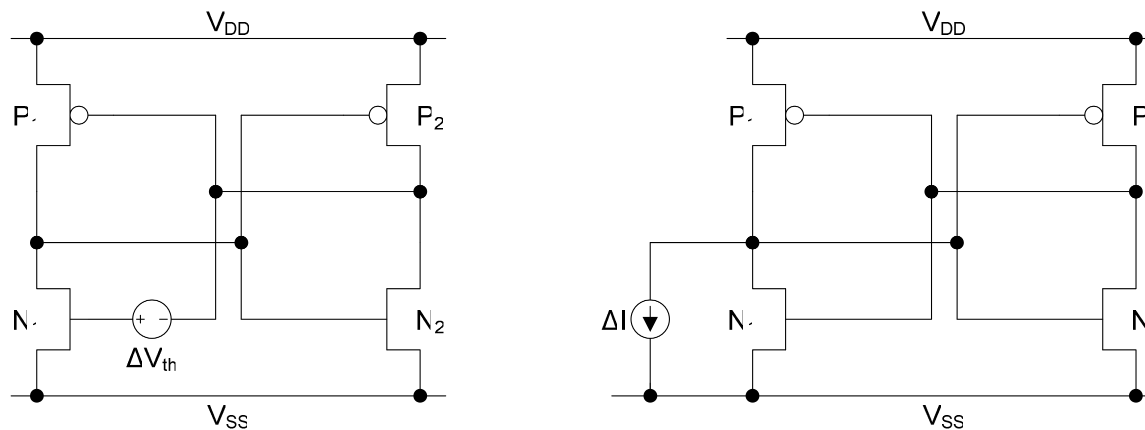
σ1 = 0.03

σ2 = 0.006 (6% error)

σ3 = σ4 = 0.001 (1% error)

At BER of 10E-10 pre-selection need 1/6 of number of cells compared to repetition code.

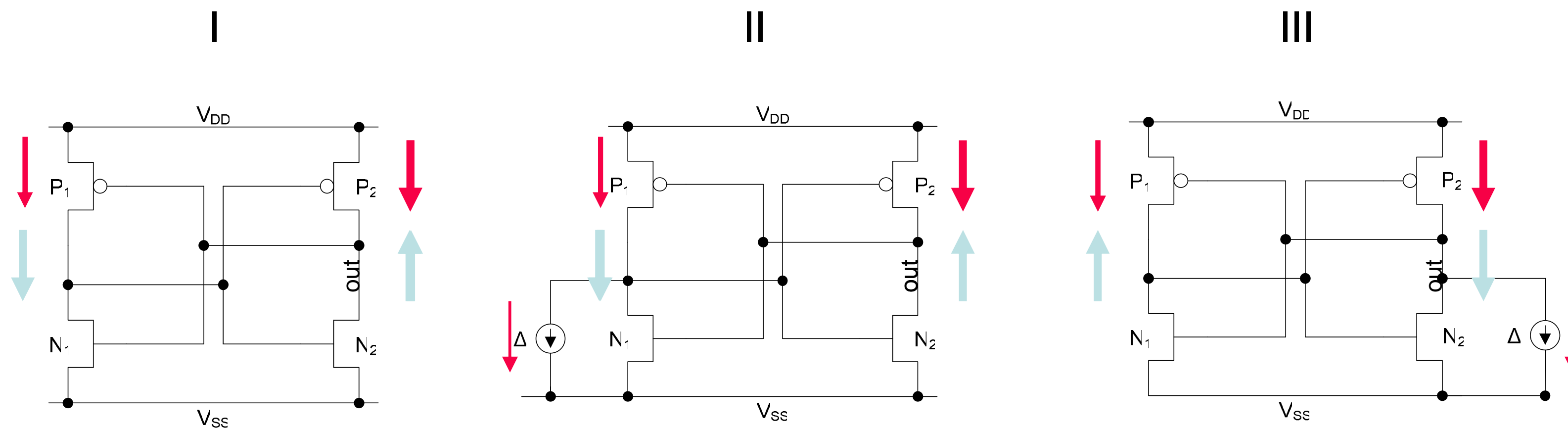
Implementation



Circuit can be implemented by either using voltage source or current source.

Implementation

Pre-selection Process:



Example:

out = 1

Mismatch is amplified:

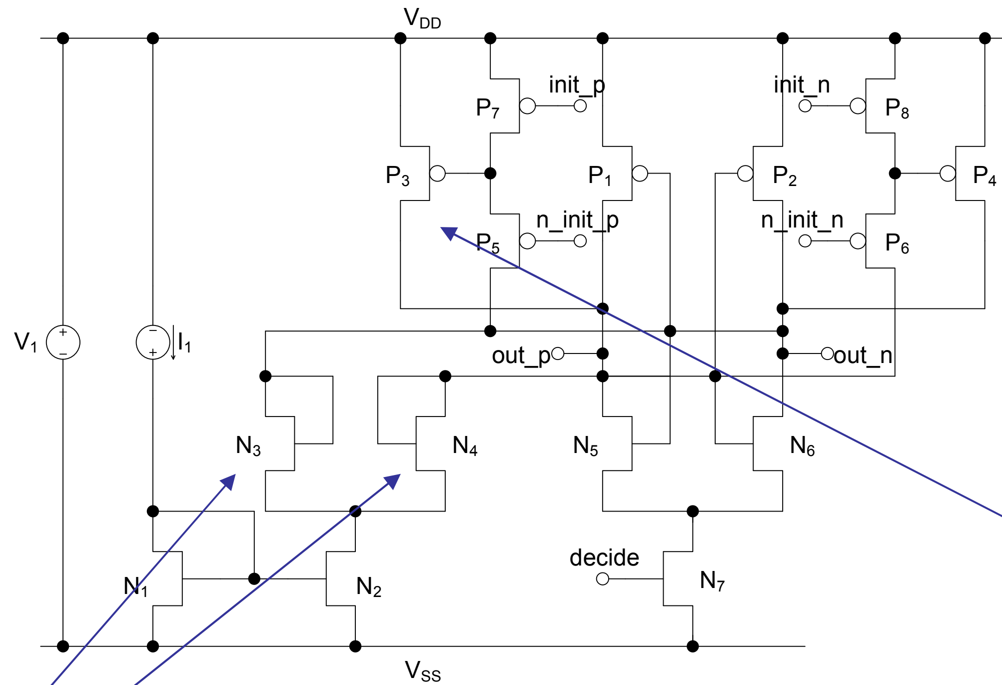
out = 1

Current source compensates mismatch:

out = 0

→ Cell is not selected

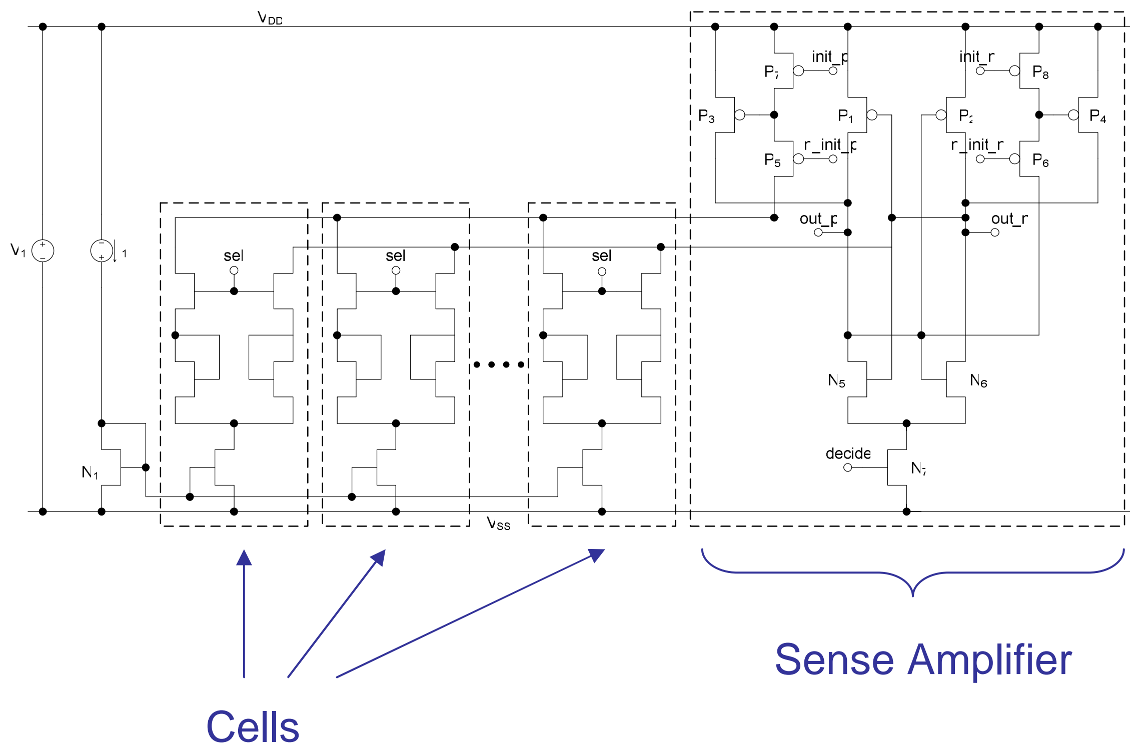
Implementation



Width extension of P1 and P2 (Current Sources)

Mismatching transistors

Sense Amplifier Sharing



- -Since sense ampl. part is quite large, area can be reduced by dividing circuit into two parts.
- -Problem: Sense amplifier has to be highly symmetrical to prevent bias in decision.

Conclusion

- SRAM-like PUF-cells exhibit high error-rates.
- Beside error correction and cell improvement, pre-selection provides solution.
- By choosing adequate threshold error-rate can be reduced significantly.
- Due to less post-processing, read-out becomes fast.
- Drawback: NVM is still needed.

Thank you for your attention!