RUHR-UNIVERSITÄT BOCHUM

RUB

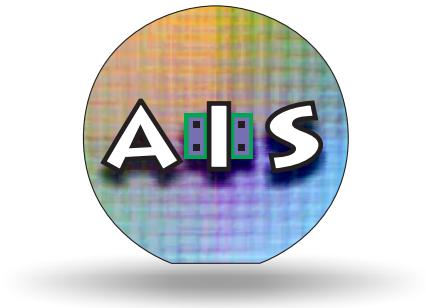
A Novel Circuit Design Methodology to Reduce Side Channel Leakage

02.11.2012

Ruhr-Universität Bochum

Analogue Integrated Circuits Research Group

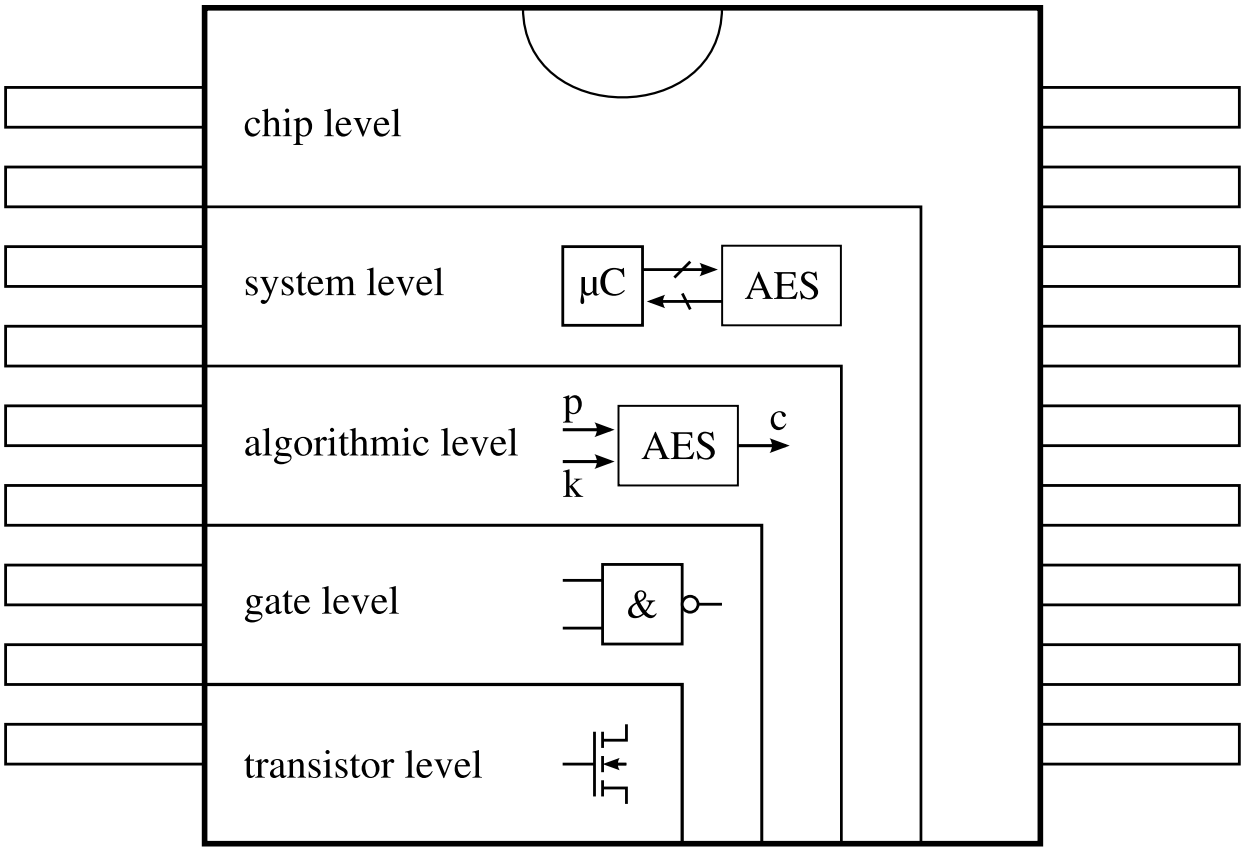
Andreas Gornik, Ivan Stoychev and Jürgen Oehm



Contents

Introduction

Design Levels for Countermeasures Against Side-Channel Leakage



[1]

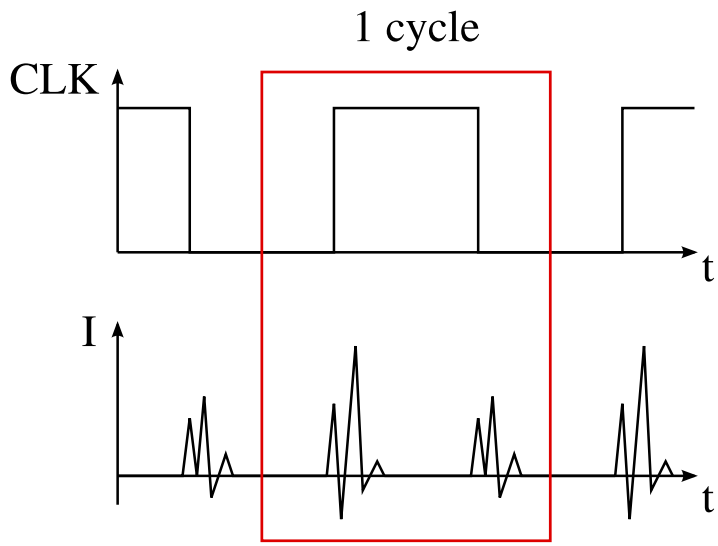
Contents

How can the Leakage be Measured? (1)

Normalized Energy Deviation (NED) [2]:

$$NED = \frac{\max(energy/cycle) - \min(energy/cycle)}{\max(energy/cycle)}$$

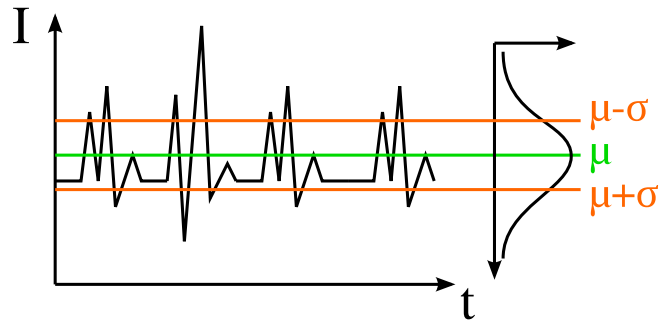
- Compares minimum/maximum energy in one cycle
  - $\Rightarrow$ Only suitable for dynamic (pre-charge) logic
- If extended to more than one cycle, only maximum and minimum energy are compared
  - $\Rightarrow$ All values in between are ignored



How can the Leakage be Measured? (2)

Normalized Standard Deviation (NSD) [2]:

$$NSD = \frac{\sigma}{\mu}$$

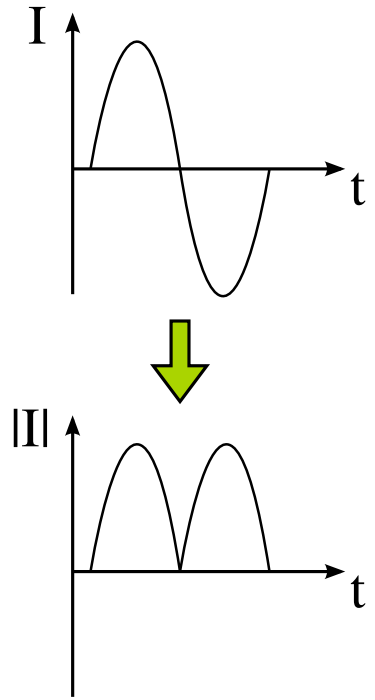


- Analyzes several clock cycles
- Based on the standard deviation σ
  - $\Rightarrow$ Cannot show the absolute difference between transitions
  - $\Rightarrow$ Switching activity of the analyzed circuit changes results
- Standard deviation σ is divided by mean μ
  - $\Rightarrow$ Large mean (generated by e.g. static current consumption) can falsify results

How can the Leakage be Measured? (3)

- Only dynamic current is considered
  - $\Rightarrow$ Static current cannot falsify results
- Dynamic current that flows into a circuit:

$$flow(X \rightarrow Y) = \int_{t_0}^{t_0+T} |I_{\mathrm{dyn}}| \, dt$$



Transition Matrix

- Matrix for all possible transitions for a 2 input gate:

$$\mathbf{T} = \begin{pmatrix} 0 \to 0 & 0 \to 1 & 0 \to 2 & 0 \to 3 \\ 1 \to 0 & 1 \to 1 & 1 \to 2 & 1 \to 3 \\ 2 \to 0 & 2 \to 1 & 2 \to 2 & 2 \to 3 \\ 3 \to 0 & 3 \to 1 & 3 \to 2 & 3 \to 3 \end{pmatrix}$$

- Example: $3 \to 2$ stands for $\binom{A}{B} = \binom{1}{1} \to \binom{1}{0}$
- Gates with 3 input signals: 8×8 matrix
  - $\Rightarrow$ Hard to compare all transitions with each other
  - $\Rightarrow$ Metric must be extended

Verbosity and Relative Verbosity (RV)

- Difference between two current peaks:

$$verbosity = \frac{1}{T} \cdot \int_{t_0}^{t_0+T} \left| |I_{\mathrm{dyn},1}| - |I_{\mathrm{dyn},2}| \right| \, dt$$

- Relative (normalized) verbosity of two current peaks:

$$RV = \frac{\int_{t_0}^{t_0+T} \left| |I_{\mathrm{dyn},1}| - |I_{\mathrm{dyn},2}| \right| \, dt}{\int_{t_0}^{t_0+T} |I_{\mathrm{dyn},1}| + |I_{\mathrm{dyn},2}| \, dt}$$

Total Relative Verbosity (TRV)

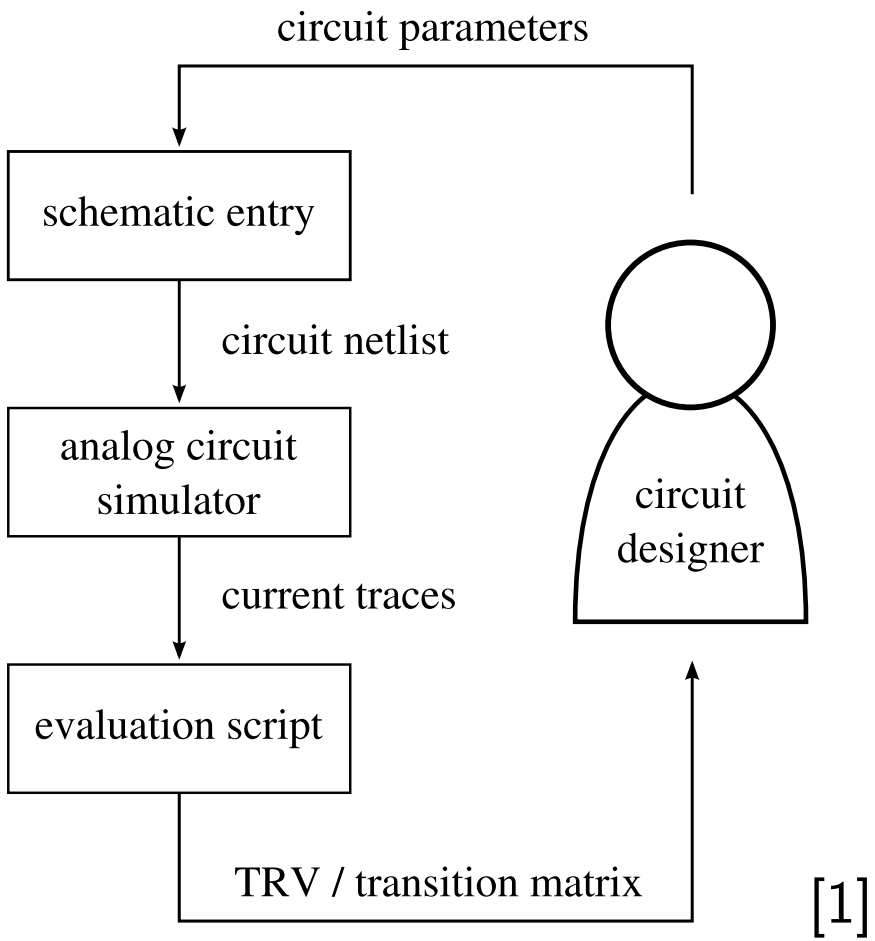
- Verbosity of all possible combinations of transitions:

$$TRV = \frac{1}{N} \cdot \sum_{i=1}^{n-1} \sum_{k=i}^{n-1} \frac{\int_{t_0}^{t_0+T} \left| |I_{\mathrm{dyn,i}}| - |I_{\mathrm{dyn,k+1}}| \right| \, dt}{\int_{t_0}^{t_0+T} |I_{\mathrm{dyn,i}}| + |I_{\mathrm{dyn,k+1}}| \, dt}$$

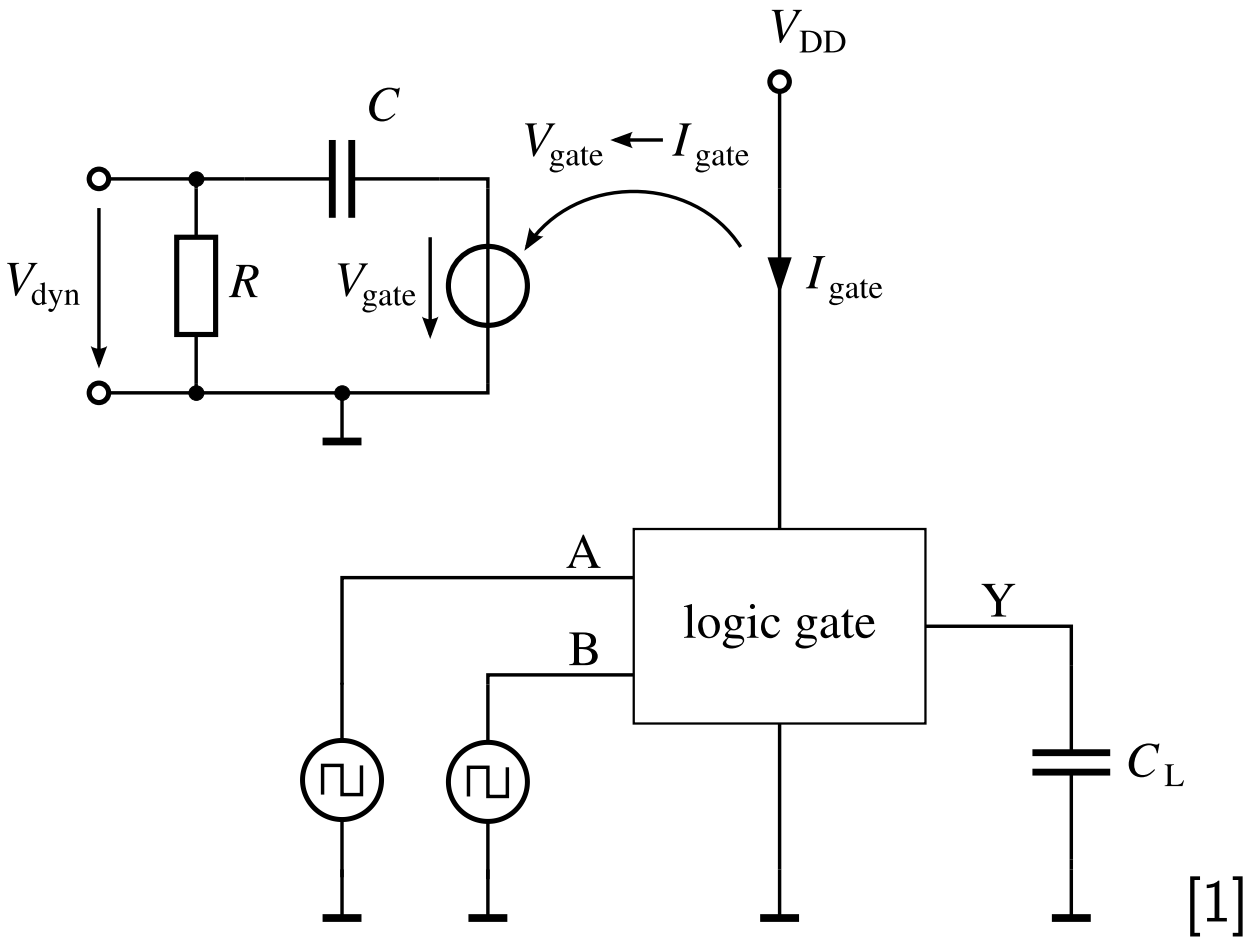
- N: number of all possible combinations of transitions
- n: number of all possible combinations of input signals

Contents

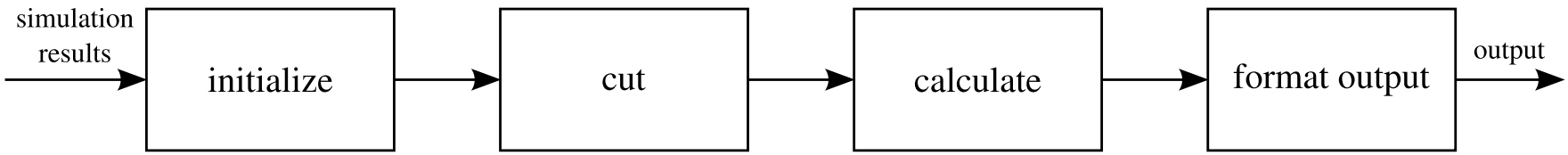
Evaluation Methodology



Test Circuit for Logic Gates



Structure of the Used Evaluation Script



[1]

- Only simulators with equally spaced time steps can be used
- Script output: *TRV* and transition matrix **T**

Contents

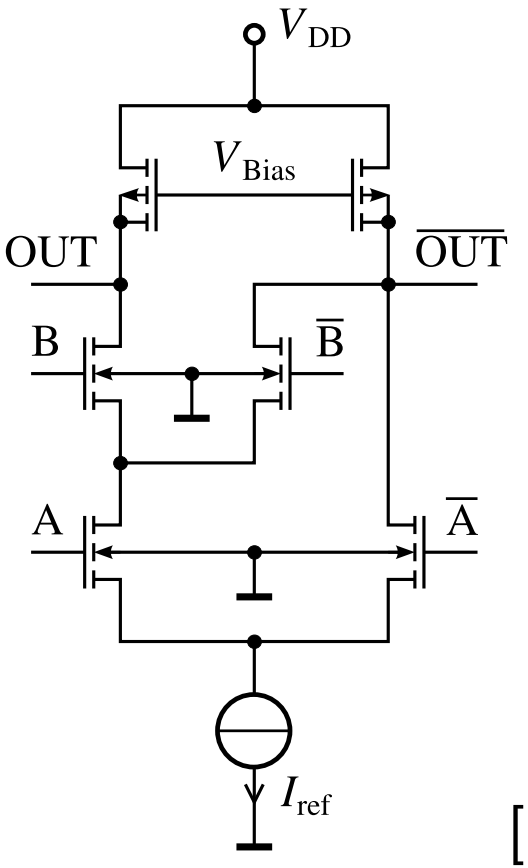
Evaluation Results

	TRV / dB		
logic circuit	CMOS	STSCL	CRSABL
2 input NAND	-5.255	-8.992	-22.655
2 input NOR	-5.031	-8.995	-23.129
AO21	-6.730	-7.780	-24.374
AO31	-7.678	-7.394	-26.495
MAOI	-7.896	-8.461	-25.047
MOAI	-7.785	-8.484	-25.894
S-Box	-7.956	-10.167	-27.014

[1]

Contents

Asymmetric 2 Input STSCL NAND

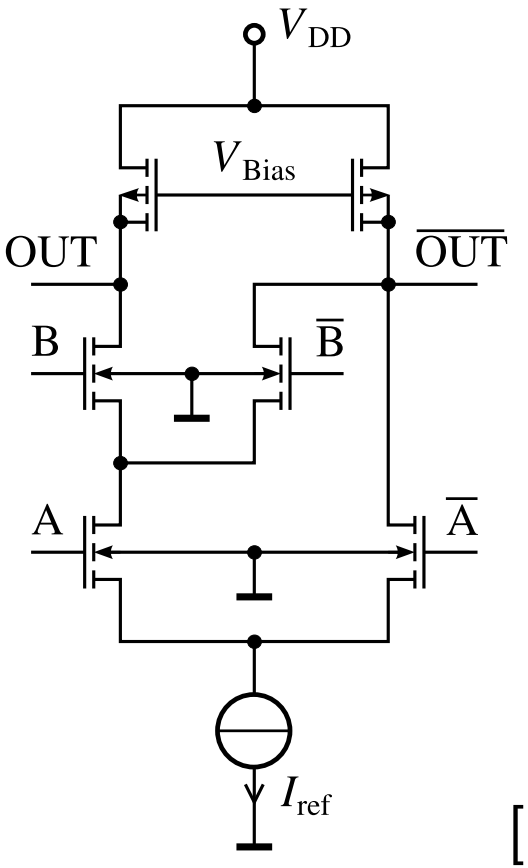


[1]

$$\mathbf{T} = \begin{pmatrix} 0 & 0.59 & 2.34 & 3.57 \\ 0.54 & 0 & 2.58 & 3.25 \\ 2.15 & 3.93 & 0 & 3.22 \\ 3.69 & 2.20 & 2.98 & 0 \end{pmatrix} \cdot 10^{-7}$$

$$TRV_{\text{asym}} = -6.81\,\text{dB}$$

Asymmetric 2 Input STSCL NAND

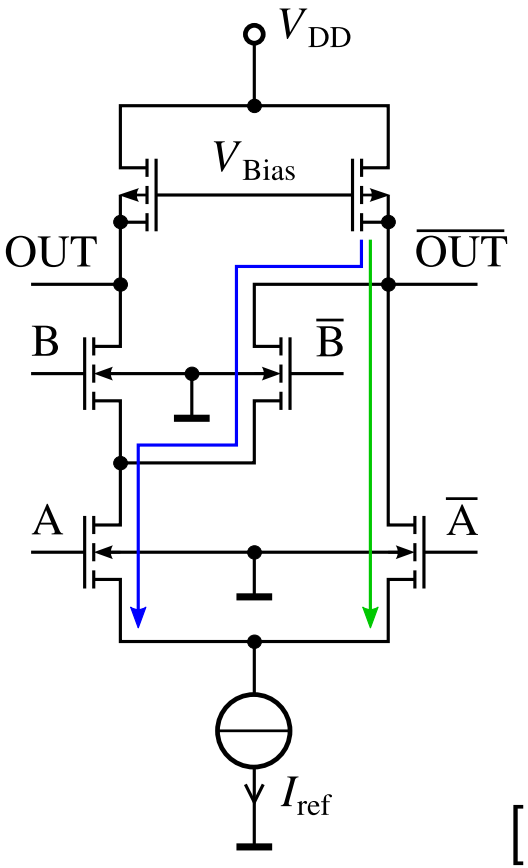


[1]

$$\mathbf{T} = \begin{pmatrix} 0 & 0.59 & 2.34 & 3.57 \\ 0.54 & 0 & 2.58 & 3.25 \\ 2.15 & 3.93 & 0 & 3.22 \\ 3.69 & 2.20 & 2.98 & 0 \end{pmatrix} \cdot 10^{-7}$$

$$TRV_{\text{asym}} = -6.81\,\text{dB}$$

Asymmetric 2 Input STSCL NAND



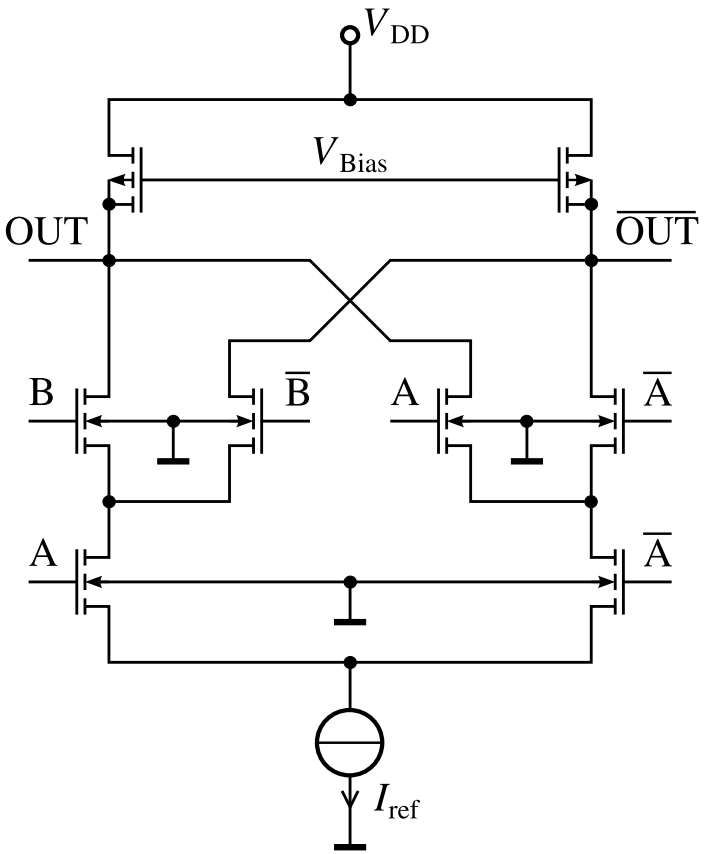
[1]

$$\mathbf{T} = \begin{pmatrix} 0 & 0.59 & 2.34 & 3.57 \\ 0.54 & 0 & 2.58 & 3.25 \\ 2.15 & 3.93 & 0 & 3.22 \\ 3.69 & 2.20 & 2.98 & 0 \end{pmatrix} \cdot 10^{-7}$$

$$TRV_{\text{asym}} = -6.81\,\text{dB}$$

$$\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Output-Symmetric 2 Input STSCL NAND



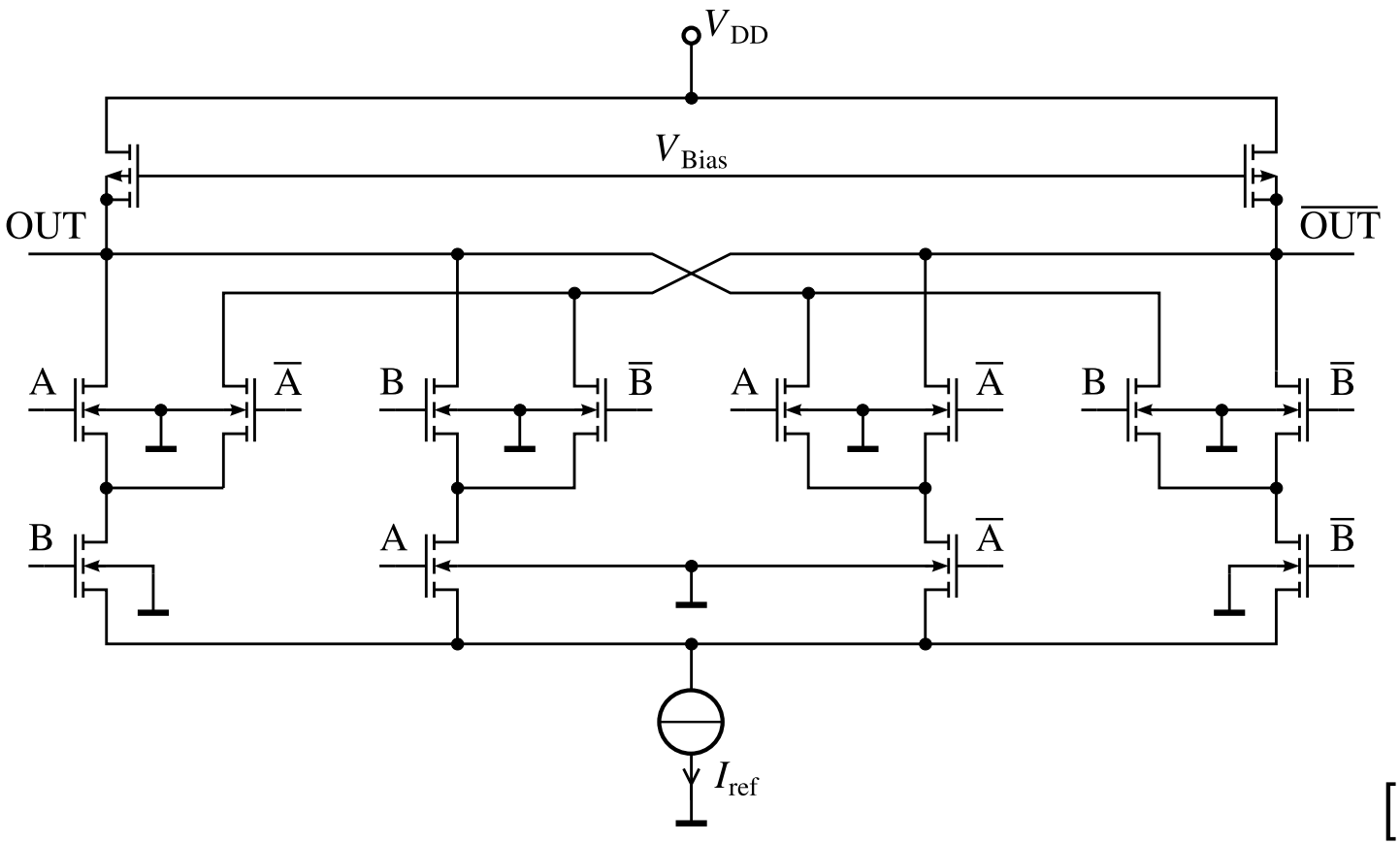
[1]

$$\mathbf{T} = \begin{pmatrix} 0 & 0.56 & 2.81 & 3.39 \\ 0.51 & 0 & 2.81 & 3.08 \\ 2.20 & 2.76 & 0 & 2.90 \\ 3.30 & 2.86 & 2.90 & 0 \end{pmatrix} \cdot 10^{-7}$$

$$TRV_{\mathrm{asym}} = -6.81\,\mathrm{dB}$$

$$TRV_{\mathrm{osym}} = -7.13\,\mathrm{dB}$$

Symmetric 2 Input STSCL NAND



[1]

Symmetric 2 Input STSCL NAND

Transition matrix:

$$\mathbf{T} = \begin{pmatrix} 0 & 1.04 & 1.02 & 3.11 \\ 0.97 & 0 & 2.31 & 2.67 \\ 0.97 & 2.32 & 0 & 2.67 \\ 3.10 & 2.23 & 2.21 & 0 \end{pmatrix} \cdot 10^{-7}$$

$$TRV_{\mathrm{asym}} = -6.81\,\mathrm{dB}$$
$$TRV_{\mathrm{osym}} = -7.13\,\mathrm{dB}$$
$$TRV_{\mathrm{sym}} = -8.99\,\mathrm{dB}$$

Contents

Conclusion & Outlook

Conclusion:

- New methodology is able to characterize side channel leakage on the transistor level
  - For a gate: TRV
  - For a transition: transition matrix
- Results show the same tendency for leakage as other methodologies
- Methodology helps circuit designers to fine-tune circuits

Outlook:

- Extend methodology for non constant power supply
- Take mismatch effects into account

Thank you for your attention.

[1] Gornik, A., Stoychev, I., Oehm, J.:
A Novel Circuit Design Methodology to Reduce Side Channel Leakage.
In Bogdanov, A., Sanadhya, S., eds.: Security, Privacy, and Applied Cryptography Engineering. Lecture Notes in Computer Science. Springer Berlin Heidelberg (2012) 1–15

[2] Kris Tiri, Moonmoon Akmal, Ingrid Verbauwhede:
A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards.
In: Proceedings of the 29th European Solid-State Circuits Conference - ESSCIRC 2002. (2002) 403–406