Information Theoretic Evaluation of Side-Channel Resistant Logic Styles

F. Macé , F.-X. Standaert , J.-J. Quisquater

UCL Crypto Group
Microelectronics Laboratory
Catholic University of Louvain - UCL
Belgium

CHES 2007

Outline

Side Channel Attacks

Side-Channel Attacks

Information gained from the physical implementation of a cryptosystem.

- On a great variety of algorithms
- On a great variety of platforms
- Using different information sources (timing, power, EM,...)

SCA Countermeasures

Existence of SW or HW based countermeasures

SW

- frequently based on time/data randomization
- easy to implement
- extensively studied

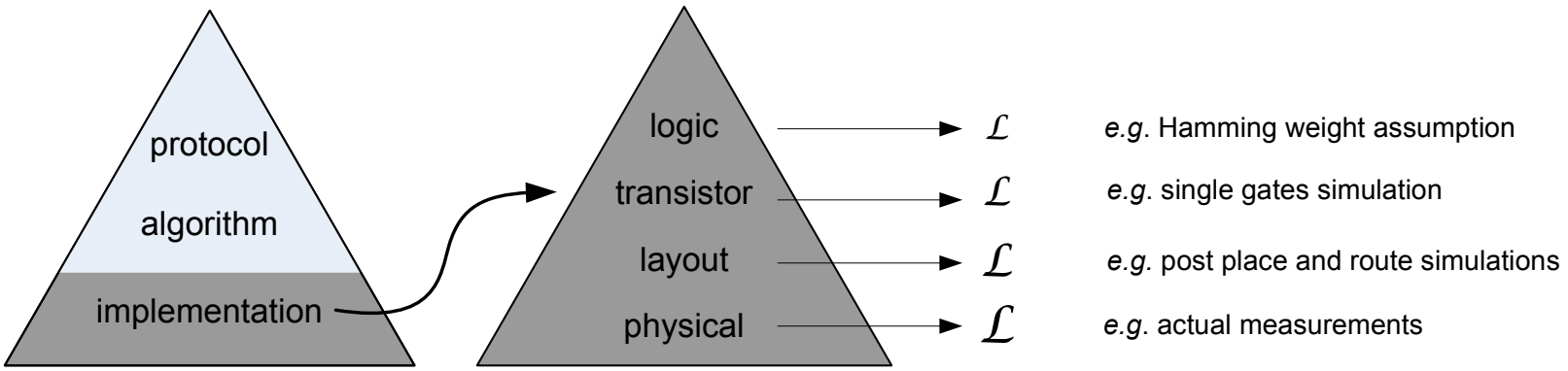
HW

$\sim$ modification of the physical structure, e.g at gate level :

- asynchronous designs
- dual-rail precharge (DRP) logic styles
- masked logic styles
- mix of DRP and masking

$\longrightarrow$ associated cost to design & test (i.e. for security)

Abstraction Layers



Circuit abstraction levels $\Leftrightarrow$ useful for a simulation based approach

Limit due to :
Going deeper in the abstraction levels $\Rightarrow$ different amount of information due to more realistic scenarios.

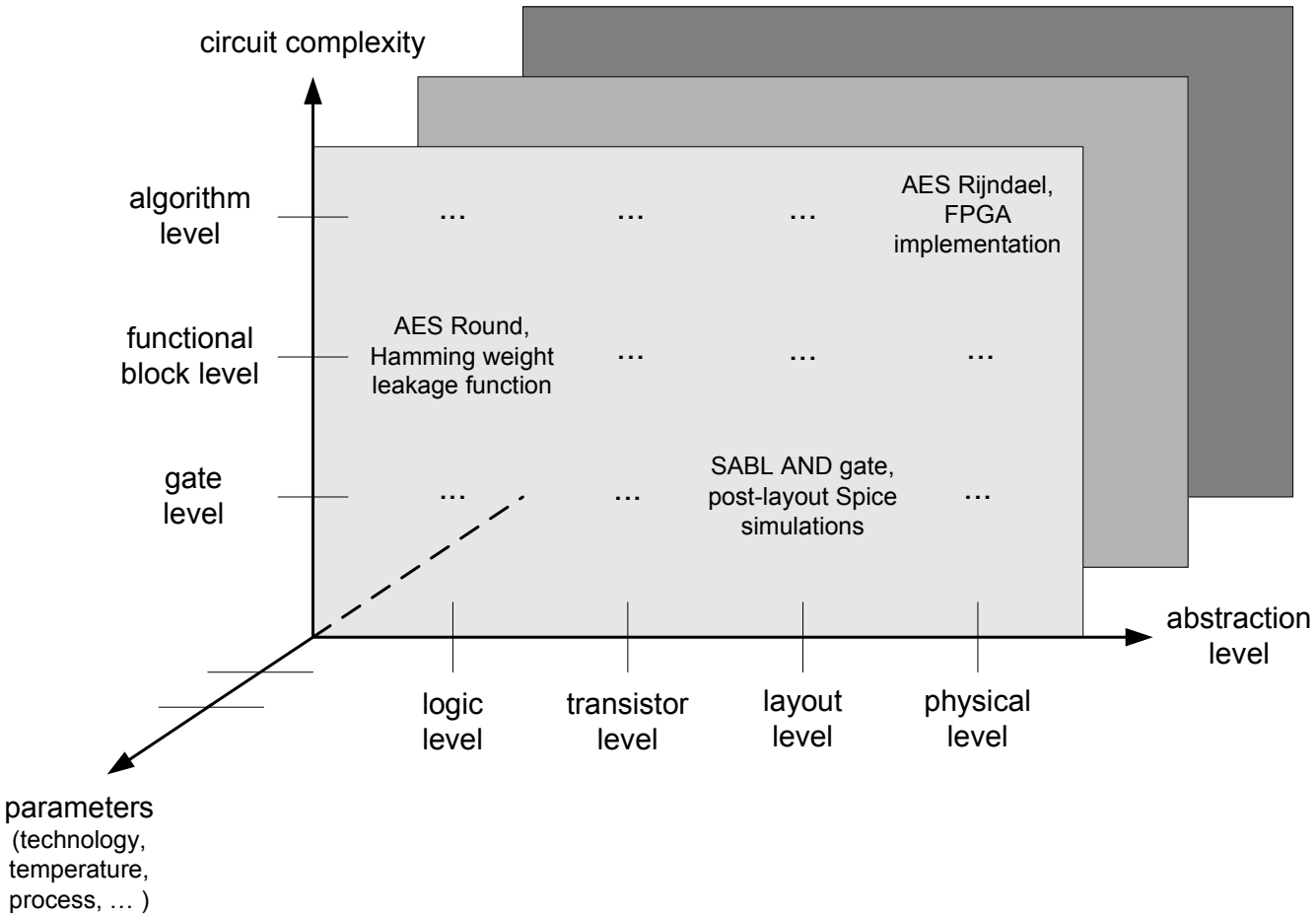
Physical level is better but simulation approach not meaningless.

Motivations

- Security evaluation methodology
- Unified evaluation metrics
- 1^{st} step : simulation based analysis, transistor level, single gates.

Methodology – 1

Assessment is multidimensional problem



Interest for a bottom - up approach.

Methodology – 2

Combination of security and information theoretic metrics [Stand06-IACR eprint]

Security Metrics

Strength of the adversary (Success rate)

Information Theoretic Metric

- Amount of leaked information (Mutual Information)
- Corresponds to the asymptotic success rate of a Bayesian adversary $\Rightarrow$ focus on it in this preliminary step

This Work $\longrightarrow 1^{st}$ Step

- discriminating different implementation $\Rightarrow$ Information

Practical Aspects - 1 : Mutual Information Computation

Notations

- S_g random variable denoting the correct target signal
- $\mathbf{L}_{s_g}^q$ a random vector containing q side-channel observations generated by s_g
- Mutual Information : $\mathrm{I}(S_g; \mathbf{L}_{s_g}^q) = \mathrm{H}[S_g] - \mathrm{H}[S_g|\mathbf{L}_{s_g}^q]$ where $\mathrm{H}[S_g]$ is the entropy of the key class S_g

$\mathrm{H}[S_g|\mathbf{L}_{s_g}^q]$ is dependant on the behavior of the implementation/countermeasure

Practical Aspects - 2 : Mutual Information Computation

Actual Computation

DRP with no mask $\rightarrow$ direct link to key

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \int \Pr[\mathbf{l}^q|s_g] \cdot \log_2 \frac{\Pr[\mathbf{l}^q|s_g]}{\sum_s \Pr[\mathbf{l}^q|s]}\ dl$$

No pre-charge/no mask $\rightarrow$ key + transition (known)

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \sum_t \Pr[t] \int \Pr[\mathbf{l}^q|s_g, t] \cdot \log_2 \Pr[\mathbf{l}^q|s_g, t]\ dl$$

Pre-charge and mask $\rightarrow$ key + mask (unknown)

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \sum_m \Pr[m] \int \Pr[\mathbf{l}^q|s_g, m] \cdot \log_2 \sum_m \Pr[\mathbf{l}^q|s, m] \cdot \Pr[m]\ dl,$$

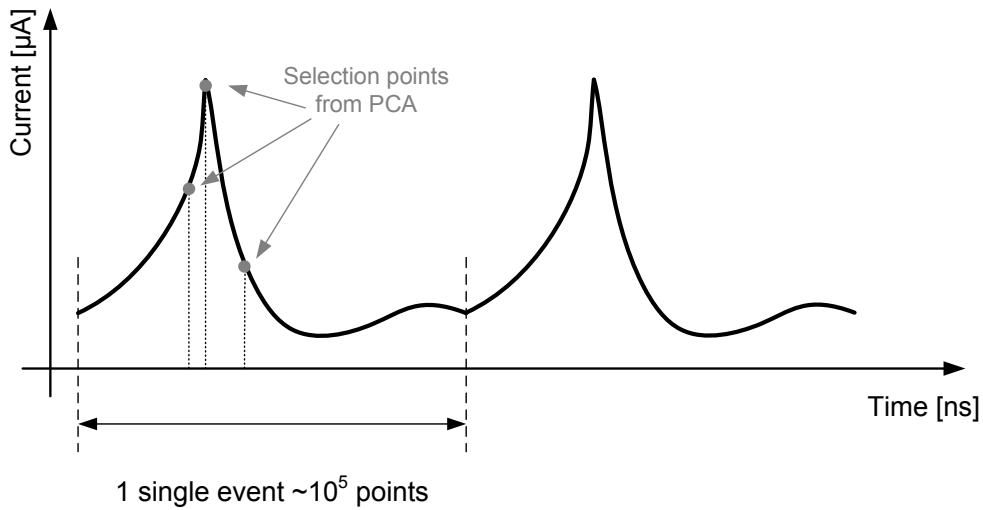
Practical Aspects - 3 : Leakage exploitation

$\neq$ Abstraction level $\leftrightarrow \neq$ leakages generated (toggle count, power traces, ...)

Power Traces

- $\mathbf{I}_{sg}^{q}$ $\rightarrow$ high dimension data ($> 10^5$ points)
- Principal Component Analysis (PCA) $\rightarrow$ reduce the high dimensionality [Arch06]

- Statistical tool for dimensionality reduction
- Preserves inter-class variance
- Good results in practice



Simulation Environment

Setup

- $0.13\mu m$ Bulk CMOS Technology (1.2V)
- BSIM3 model from measurements.
- Simulation on ELDO
- Time resolution 10^{-4} *ns*
- DRP logic styles, masks, full-custom, Std cell based

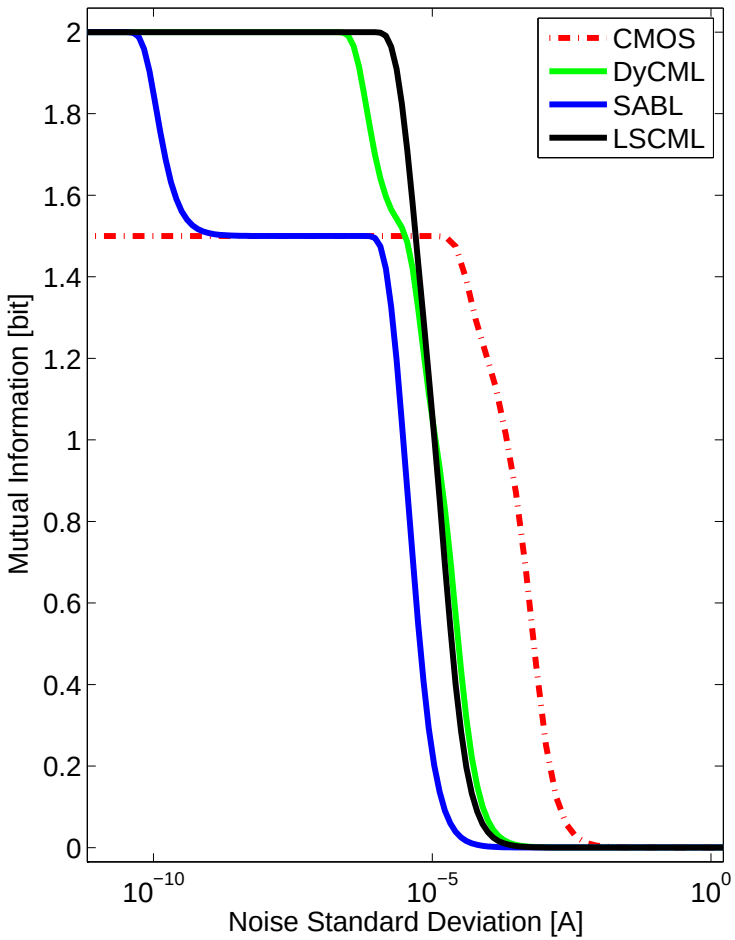
Evaluated functions

AN2,OR2,AN3,OR3,XOR2,MAJ

Illustration - 1

Existence of undistinguishable leakages

AN2 Gate



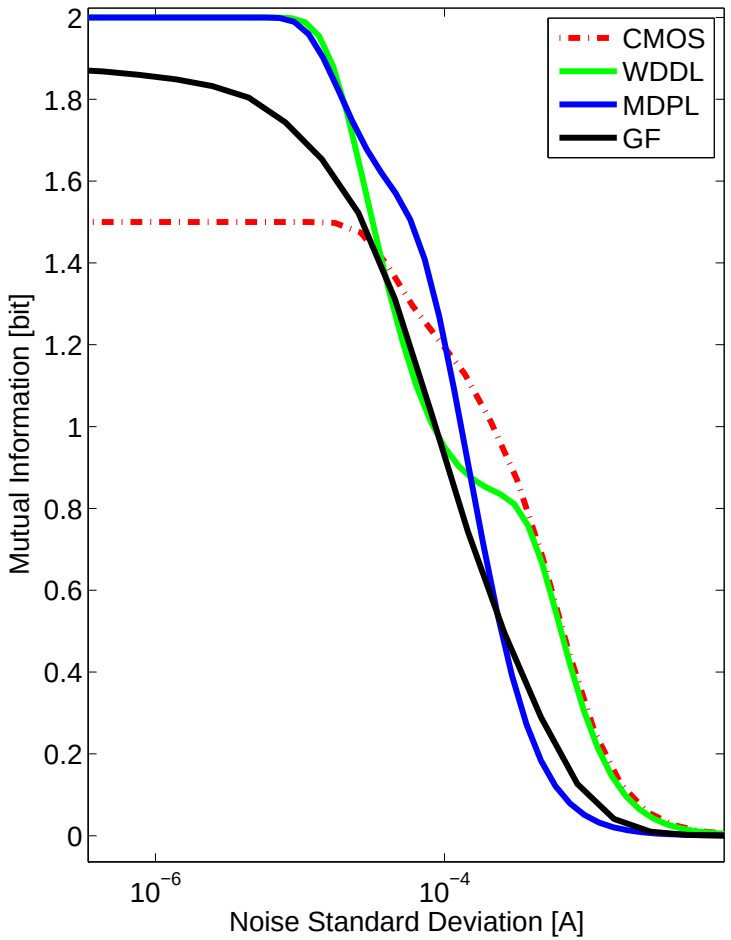
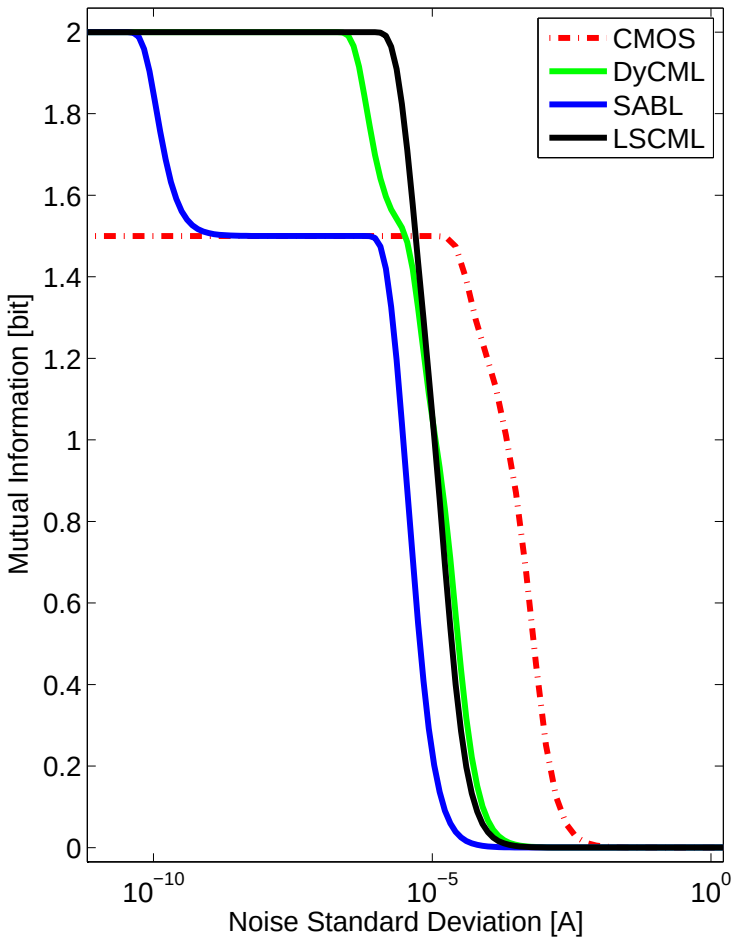


Illustration - 2

Comparison results dependant on the noise variance

Masked vs DRP $\longrightarrow$ variance based comparison is meaningless

AN2 Gate



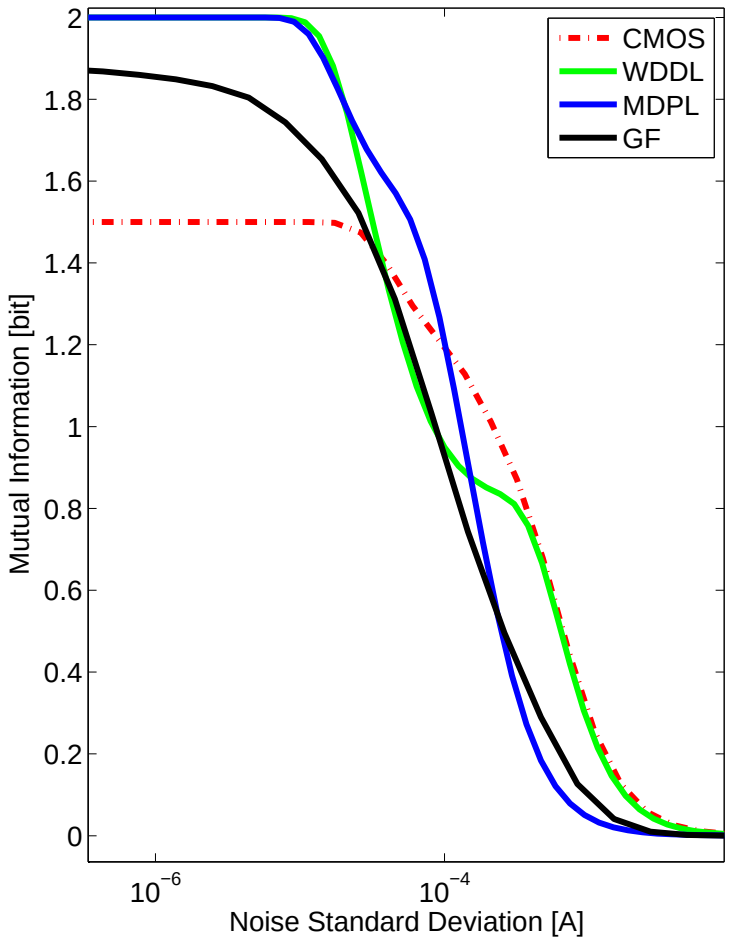
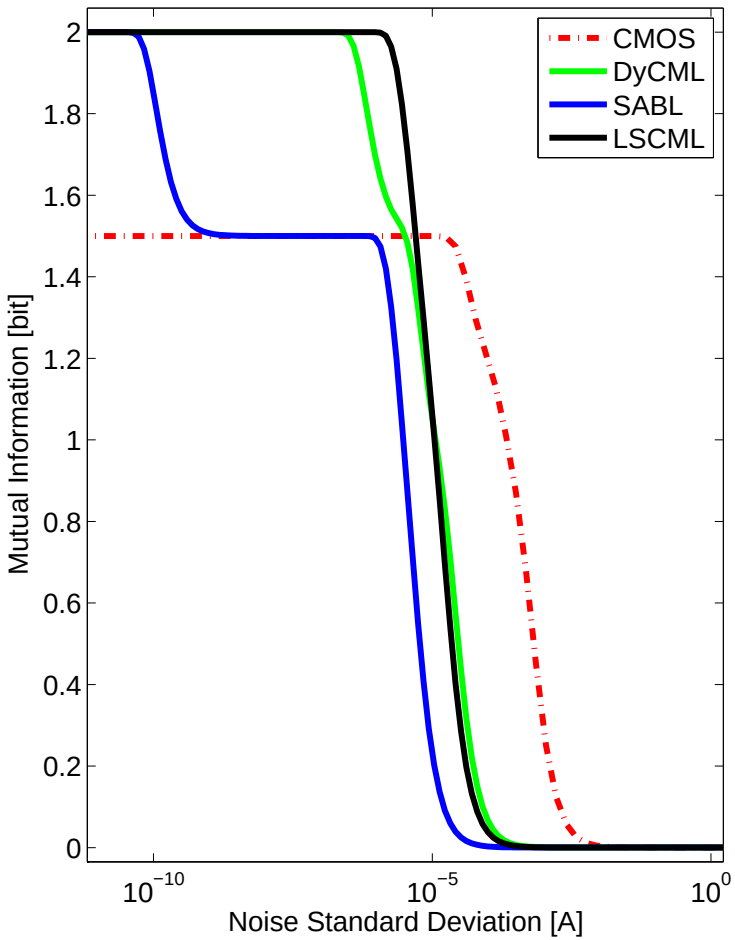
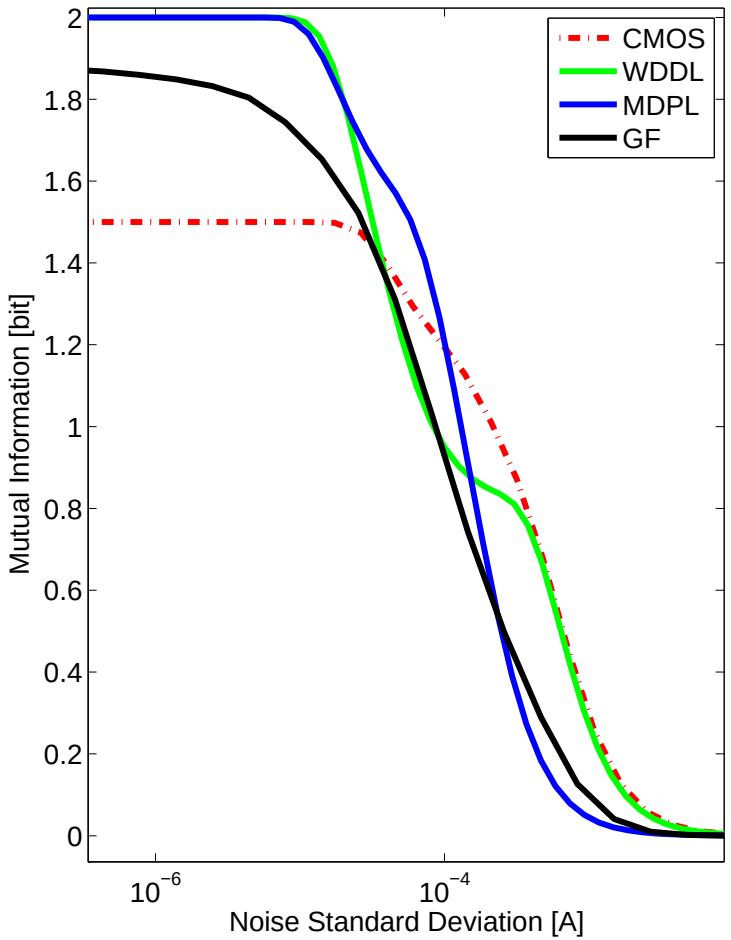


Illustration- 3

Full custom logic allows quicker reduction of information

AN2 Gate





Conclusions

Black Box Analysis

Methodology bridges the gap between algorithmic design issues and physical origins of the leakages

Unified Methodology

Applicable to any working principle of the countermeasures, at any circuit level or complexity, for any side-channel

Limitations

Methodology not limited by its own principle but by the extent to which the statistical tool correctly extracts leakage points

Further Work

- Explore different circuit complexity
- Apply the methodology to different abstraction levels
- Determine the impact of other parameters (temperature, technology, ...)
- Existence of a better statistical tool ?
- Evaluate the link between information metrics and security metrics