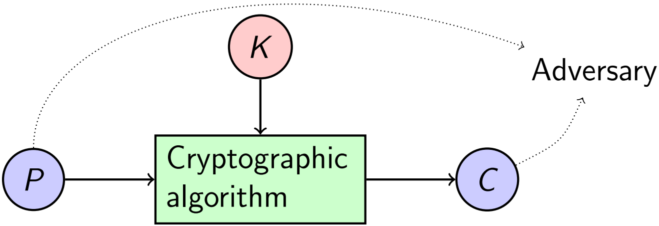
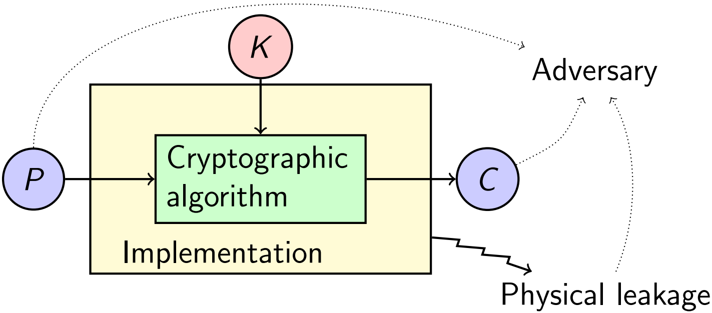
Information Theoretic and Security Analysis of a 65-nanometer DDSLL AES S-box

Mathieu Renauld, Dina Kamel, François-Xavier Standaert, Denis Flandre.

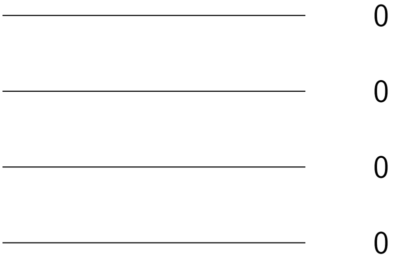
September 2011



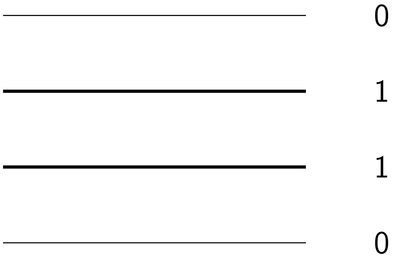
Classical cryptanalysis



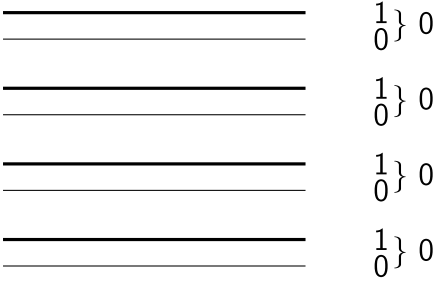
Side-Channel cryptanalysis



Standard CMOS.



Standard CMOS.



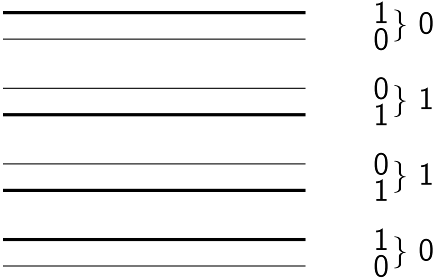
$\left.\begin{matrix}1\\0\end{matrix}\right\}0$

$\left.\begin{matrix}1\\0\end{matrix}\right\}0$

$\left.\begin{matrix}1\\0\end{matrix}\right\}0$

$\left.\begin{matrix}1\\0\end{matrix}\right\}0$

Dual-rail pre-charge logic style (DRP).



Dual-rail pre-charge logic style (DRP).

DRP main goals:

- Break the linearity of the leakage model (invalidate Hamming weight/distance model),
- Reduce the data dependency,
- Ideally, without a big performance hit.

Motivations:

1. DRP = trade off performance vs. security.
    - Previous solutions biased towards security.
    - Can we increase efficiency? At what cost?
    - DDSLL as a case study.

Motivations:

1. DRP = trade off performance vs. security.
   - Previous solutions biased towards security.
   - Can we increase efficiency? At what cost?
   - DDSLL as a case study.
2. Worst case IT analysis of a real DRP chip.

Motivations:

1. DRP = trade off performance vs. security.
   - Previous solutions biased towards security.
   - Can we increase efficiency? At what cost?
   - DDSLL as a case study.
2. Worst case IT analysis of a real DRP chip.
3. Leakage non-linearity increases the difficulty of non-profiled attacks. Does DDSLL offer this kind of protection?

Outline

Performance analysis

Side-channel attacks

- IT analysis
- Security analysis

Conclusion

Outline

Performance analysis

Side-channel attacks
- IT analysis
- Security analysis

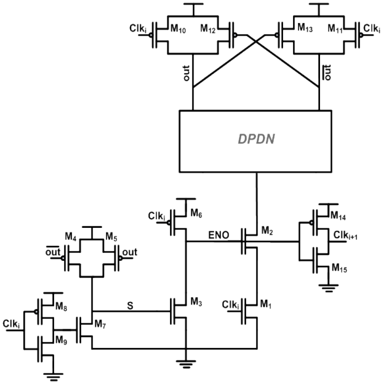
Conclusion

Performance analysis

DDSLL logic:

General characteristics

- Dynamic and differential.
- Self-timed.



Performance analysis

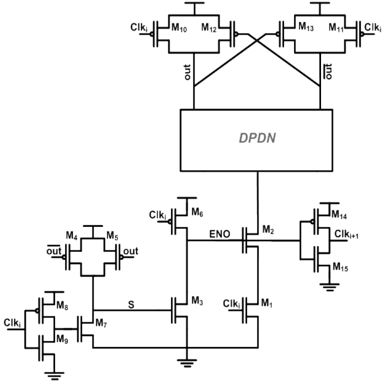
DDSLL logic:

General characteristics

- Dynamic and differential.
- Self-timed.

Performances increase

- Power: low-swing.
- Area: differential pull down network.



Performance analysis

DDSLL logic:

General characteristics

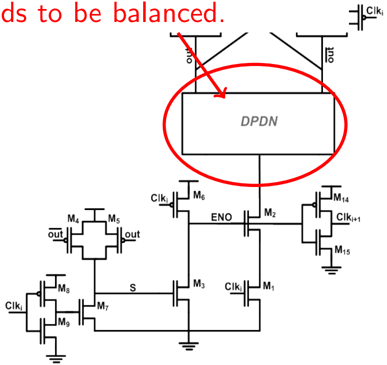
- Dynamic and differential.
- Self-timed.

Performances increase

- Power: low-swing.
- Area: differential pull down network.

Vs. security

Implements complex functions, needs to be balanced.



Performance analysis

DDSLL logic:

General characteristics

- Dynamic and differential.
- Self-timed.

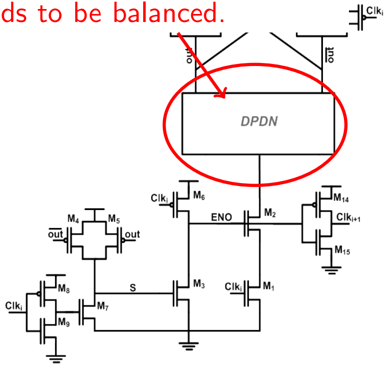
Performances increase

- Power: low-swing.
- Area: differential pull down network.

Vs. security

Full custom.

Implements complex functions, needs to be balanced.



Performance analysis

Comparison setup:

- Static CMOS vs. DDSLL AES S-box.
- Tower field architecture.
- 65-nanometer technology.
- Measurements at 1.2V supply voltage.
- Separate power supplies.

Performance analysis

Performance comparison.

S-box:	Static CMOS	DDSLL	
Area	1000 μm^2	1125 μm^2	=
Avg. power @ 100kHz	128 nW	82 nW	↘
delay	3 ns	8 ns	↗

Outline

Performance analysis

Side-channel attacks

- IT analysis
- Security analysis

Conclusion

Outline

Performance analysis

Side-channel attacks

- IT analysis
- Security analysis

Conclusion

IT analysis

$$\mathsf{MI}(X;L) = \mathsf{H}[X] - \sum_{x\in\mathcal{X}} \mathsf{Pr}[x] \sum_{l\in\mathcal{L}} \mathsf{Pr}_{\texttt{chip}}[l|x] \log_2 \hat{\mathsf{Pr}}_{\texttt{model}}[x|l]$$

IT analysis

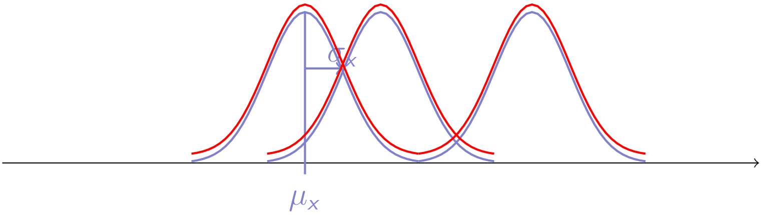
$$\mathrm{MI}(X;L) = \mathrm{H}[X] - \sum_{x\in\mathcal{X}} \Pr[x] \sum_{l\in\mathcal{L}} \Pr_{\texttt{chip}}[l|x] \log_2 \hat{\Pr}_{\texttt{model}}[x|l]$$

Interpretation:

- $\Pr_{\texttt{chip}}[l|x]$ are the pdf from the actual chip.
- $\hat{\Pr}_{\texttt{model}}[x|l]$ are the estimated pdf from the adversary's model.

IT analysis

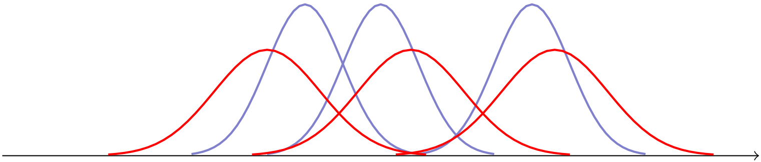
Template model



Adversary's model $\simeq$ chip leakage function.

IT analysis

Linear stochastic model



Adversary's model : $\mu_x = \sum_k \alpha_k g_k(x)$

IT analysis

2 profiled side-channel attacks ⇒ 2 adversary's models.

1. Template model.
   - Most powerful attack from the IT p.o.v. as it models perfectly the device leakage function.
2. Linear stochastic model.
   - Evaluate the linearity of the leakage function.

IT analysis

Template model,
perfect profiling phase

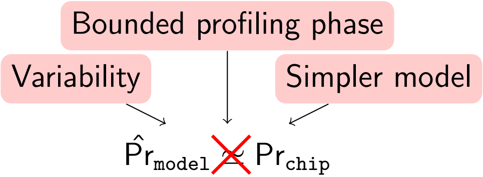
$$\downarrow$$

$$\hat{\mathrm{P}}\mathrm{r}_{\mathtt{model}} \simeq \mathrm{Pr}_{\mathtt{chip}}$$

$$\mathrm{MI}(X;L) = \mathrm{H}[X] - \sum_{x\in\mathcal{X}} \mathrm{Pr}[x] \sum_{l\in\mathcal{L}} \mathrm{Pr}_{\mathtt{chip}}[l|x] \log_2 \hat{\mathrm{P}}\mathrm{r}_{\mathtt{model}}[x|l]$$

Mutual information = worst case scenario.

IT analysis



Bounded profiling phase

Variability

Simpler model

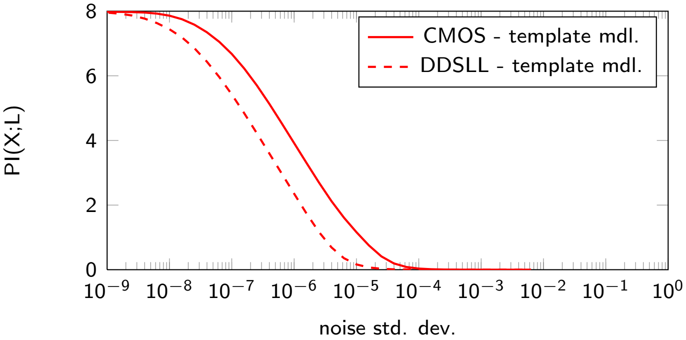
$$\hat{\mathrm{Pr}}_{\mathtt{model}} \cancel{\simeq} \mathrm{Pr}_{\mathtt{chip}}$$

$$\underset{\mathrm{PI}}{\cancel{\mathrm{MI}}}(X;L) = \mathrm{H}[X] - \sum_{x\in\mathcal{X}} \mathrm{Pr}[x] \sum_{l\in\mathcal{L}} \mathrm{Pr}_{\mathtt{chip}}[l|x] \log_2 \hat{\mathrm{Pr}}_{\mathtt{model}}[x|l]$$

Perceived information = biased evaluation.

IT analysis

IT metric: CMOS vs. DDSLL (measurements)

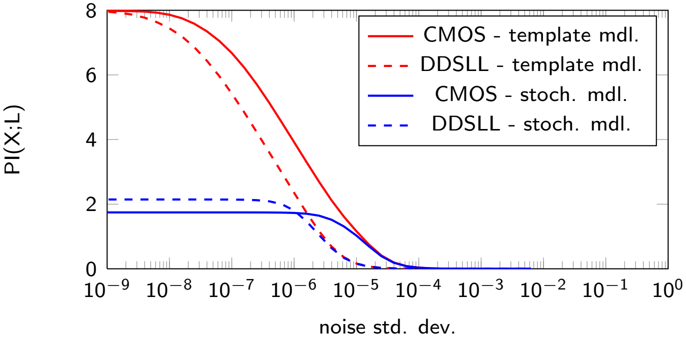


+ : the security increases with a low performance hit.

- : not sufficient as a standalone protection.

IT analysis

IT metric: CMOS vs. DDSLL (measurements)



Linearity, even for DDSLL.

.

Outline

Performance analysis

Side-channel attacks

- IT analysis
- Security analysis

Conclusion

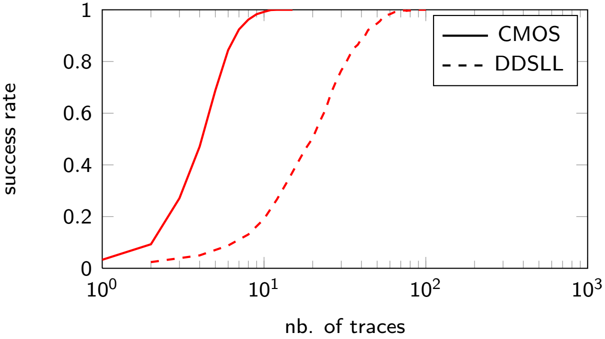
Security analysis

Security analysis:

- Metric: success rate of various profiled (template) and non-profiled (DPA, CPA, on-the-fly stochastic) attacks.
    - Template attacks are the worst-case scenario.
    - DPA, CPA are popular non-profiled attacks.
    - On-the-fly stochastic attack is the non-profiled equivalent of stochastic models (more generic than DPA and CPA).
- Attacks on different time samples.

Security analysis

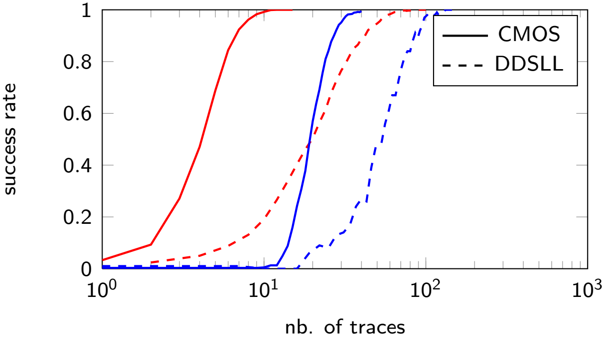
Security: CMOS vs. DDSLL. (Best time samples)



- Template attack.

Security analysis

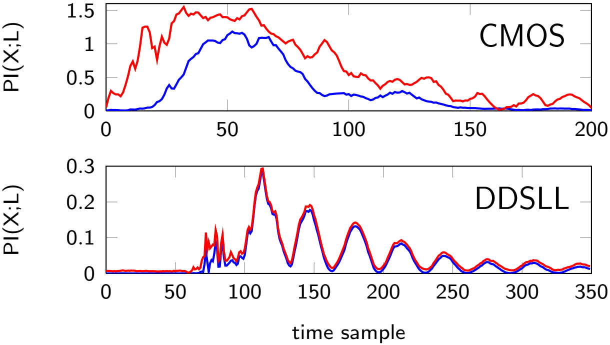
Security: CMOS vs. DDSLL. (Best time samples)



- Template attack.
- On-the-fly stochastic attack.

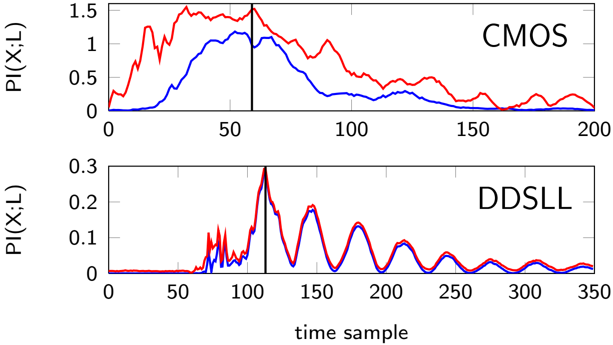
Security analysis

Time sample selection and linearity.



Security analysis

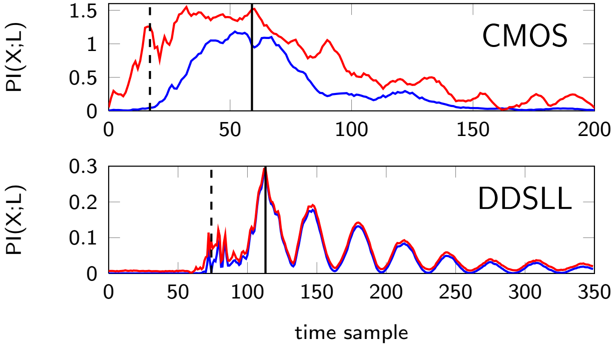
Time sample selection and linearity.



- Some time samples are accurately predicted by a linear model.

Security analysis

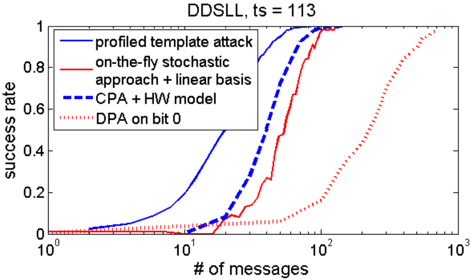
Time sample selection and linearity.



- Some time samples are accurately predicted by a linear model.
- Some are not (but still contain information!).

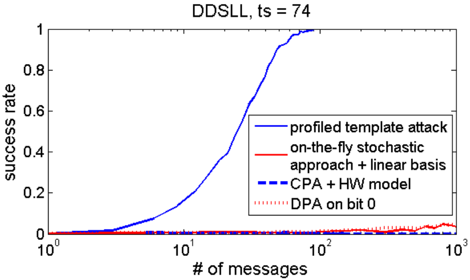
Security analysis

Some time sample are easy to exploit with non-profiled attacks...



Security analysis

...but others are too non-linear.



Outline

Performance analysis

Side-channel attacks

- IT analysis
- Security analysis

Conclusion

Conclusion

- DDSLL focuses on reducing the performance drawback,
- And offers a security improvement over CMOS,
- But information leakage remains significant.
- The leakages are more linear than expected, allowing non-profiled attacks.

Conclusion

Open questions:

- Is it possible to better balance the DPDN?
- Is DDSLL interesting combined with other SC coutermeasures?

Do our conclusions hold

- With other DRP logic styles?
- With smaller technologies?

Thank you for your attention.