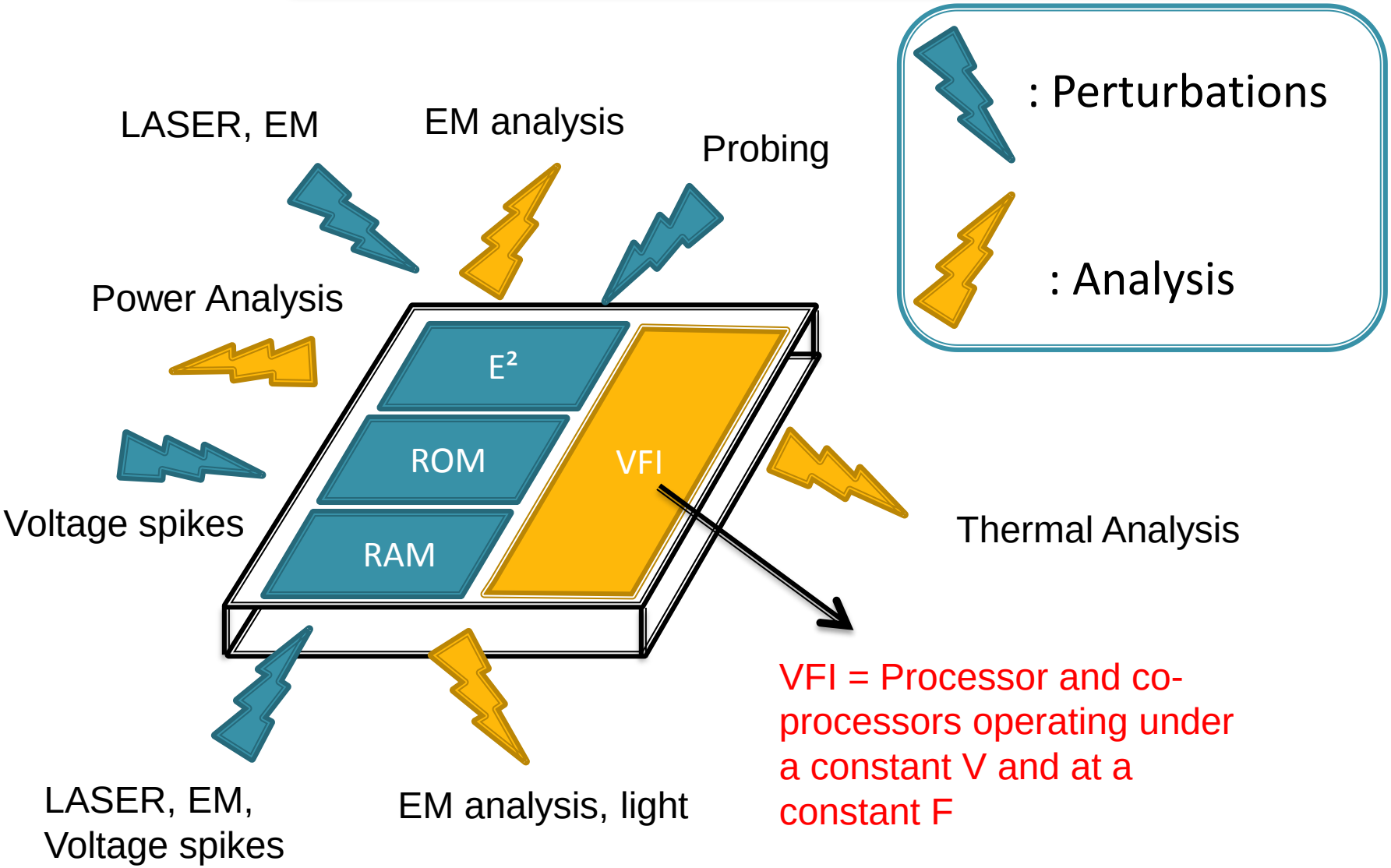
Efficiency of the Random DVFS countermeasure

S.Ordas , M.Carbone , G.Ducharme, S.Tiran, P.Maurine

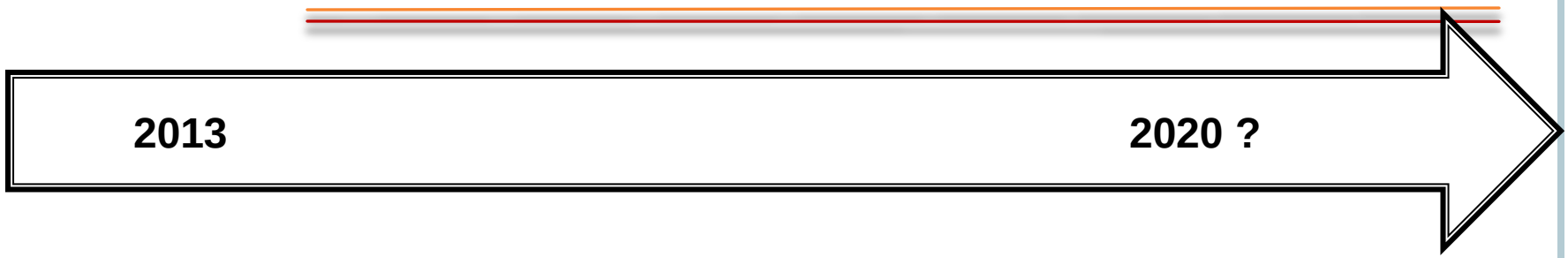
Outline

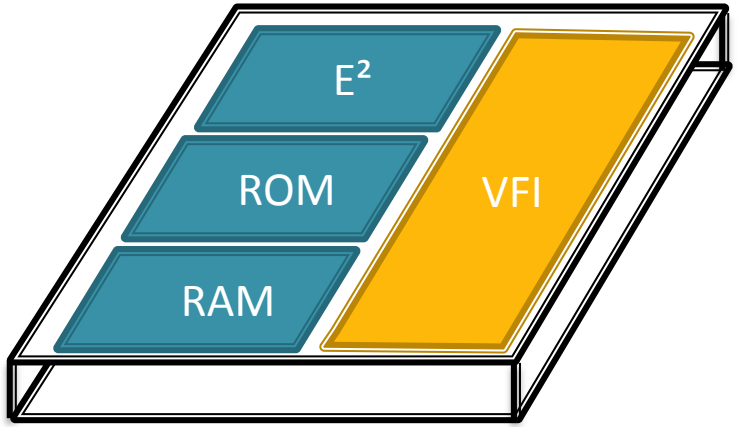
1. State of the Art
2. Effects of F and V changes on the physical leakage
3. Experimental results
4. Enhancing CPA efficiency
5. Conclusion

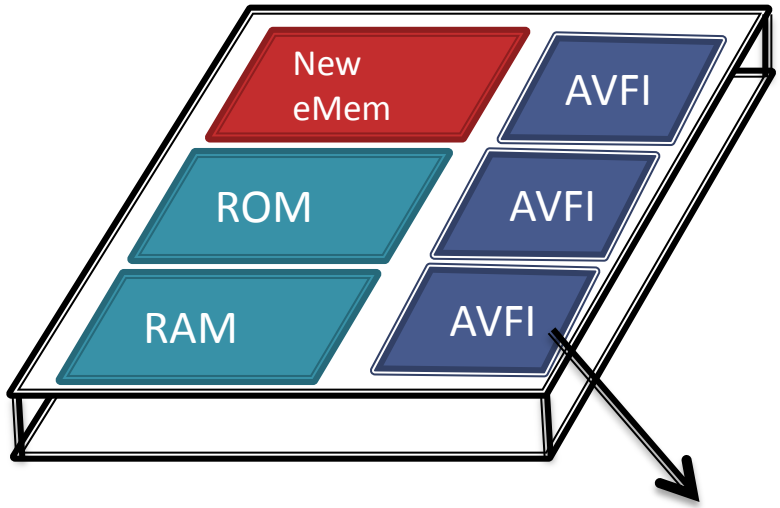
SmartCards and Side Channels



SmartCard : a trend ?







Adaptive Voltage and Frequency Island

Design Challenges (leakage power, Design for Yield, intra die process variations) ---> DVFS

Motivations

- Trading performances (Speed and Power) for security?
- Impact of the voltage changes against Side Channels Attacks ?
- Impact of the frequency changes against Side Channels Attacks ?

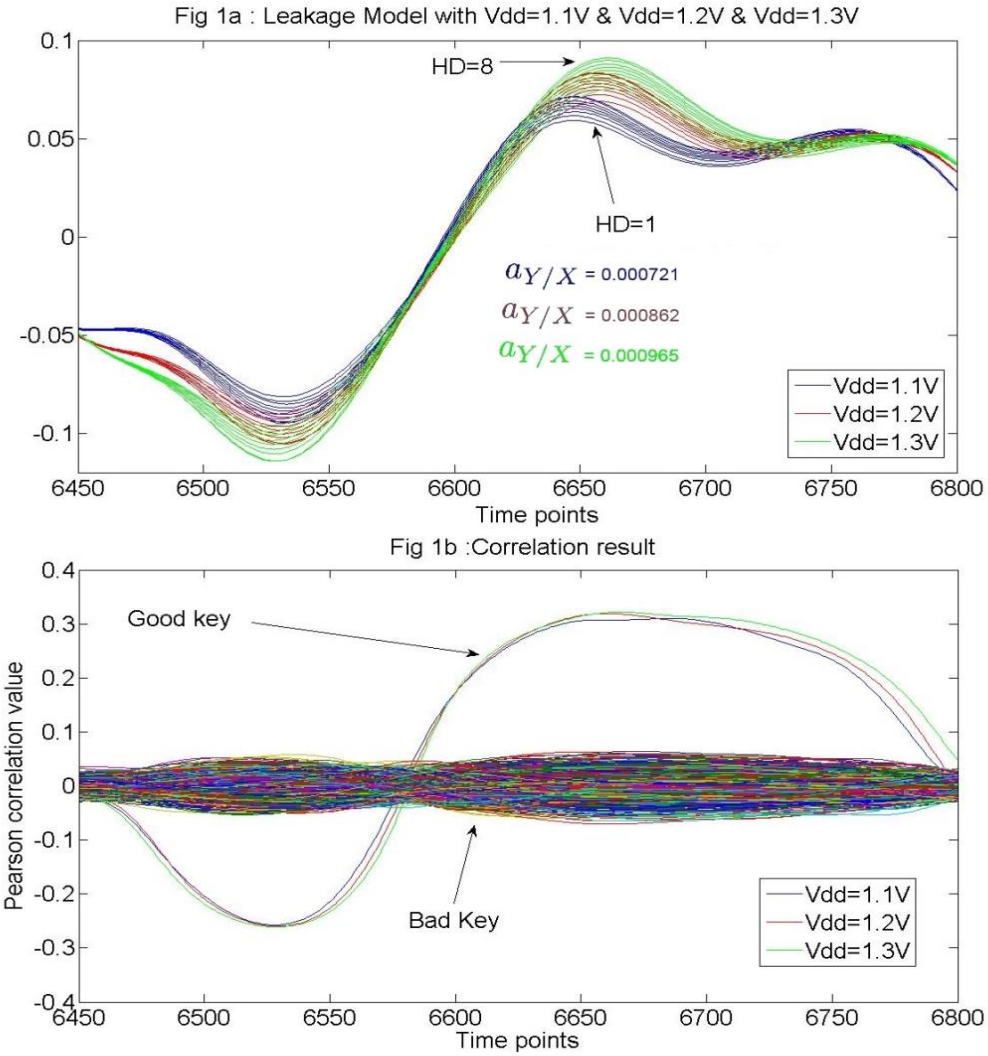
State of the Art

1999 — P. C. Kocher, J. Jaffe, and B. Jun,
"Differential power analysis"

2005 — S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie
"Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach"

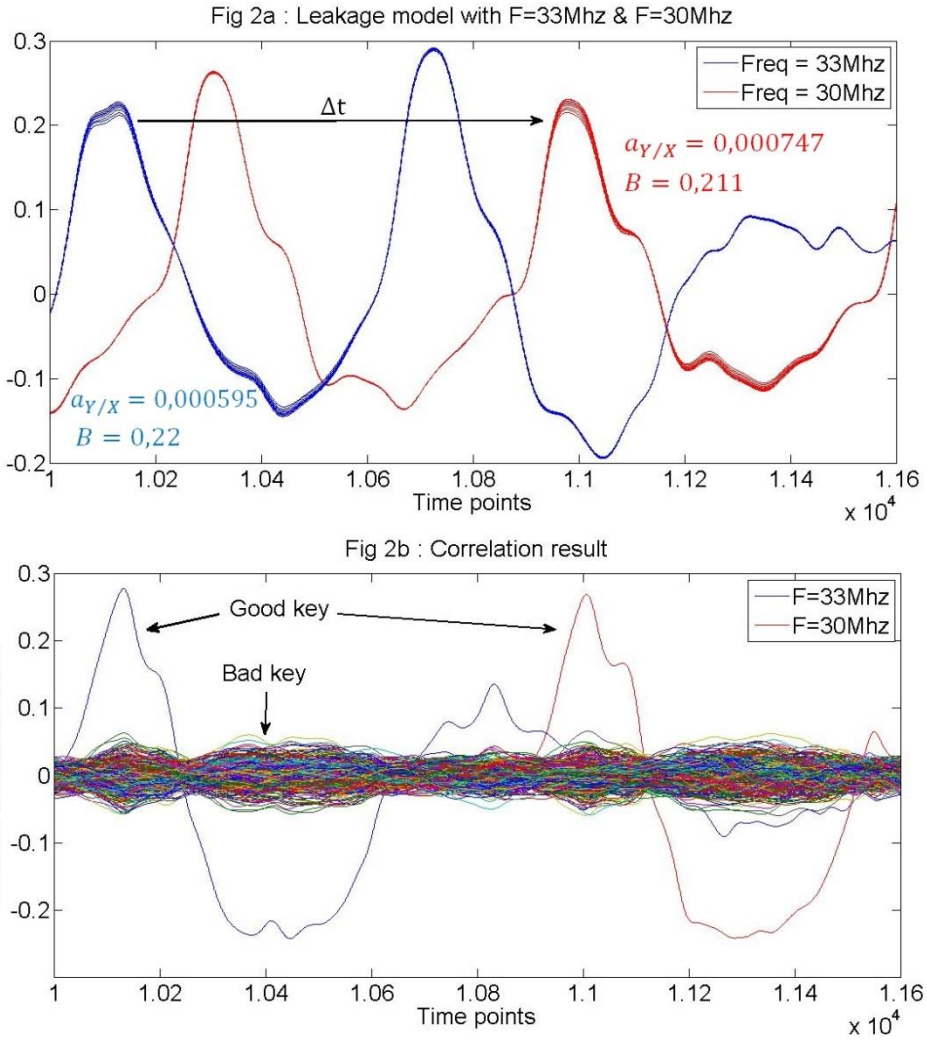
2007 — K. Baddam, M. Zwolinski
"Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure"

Effect of changes in Voltage (Random DVS)



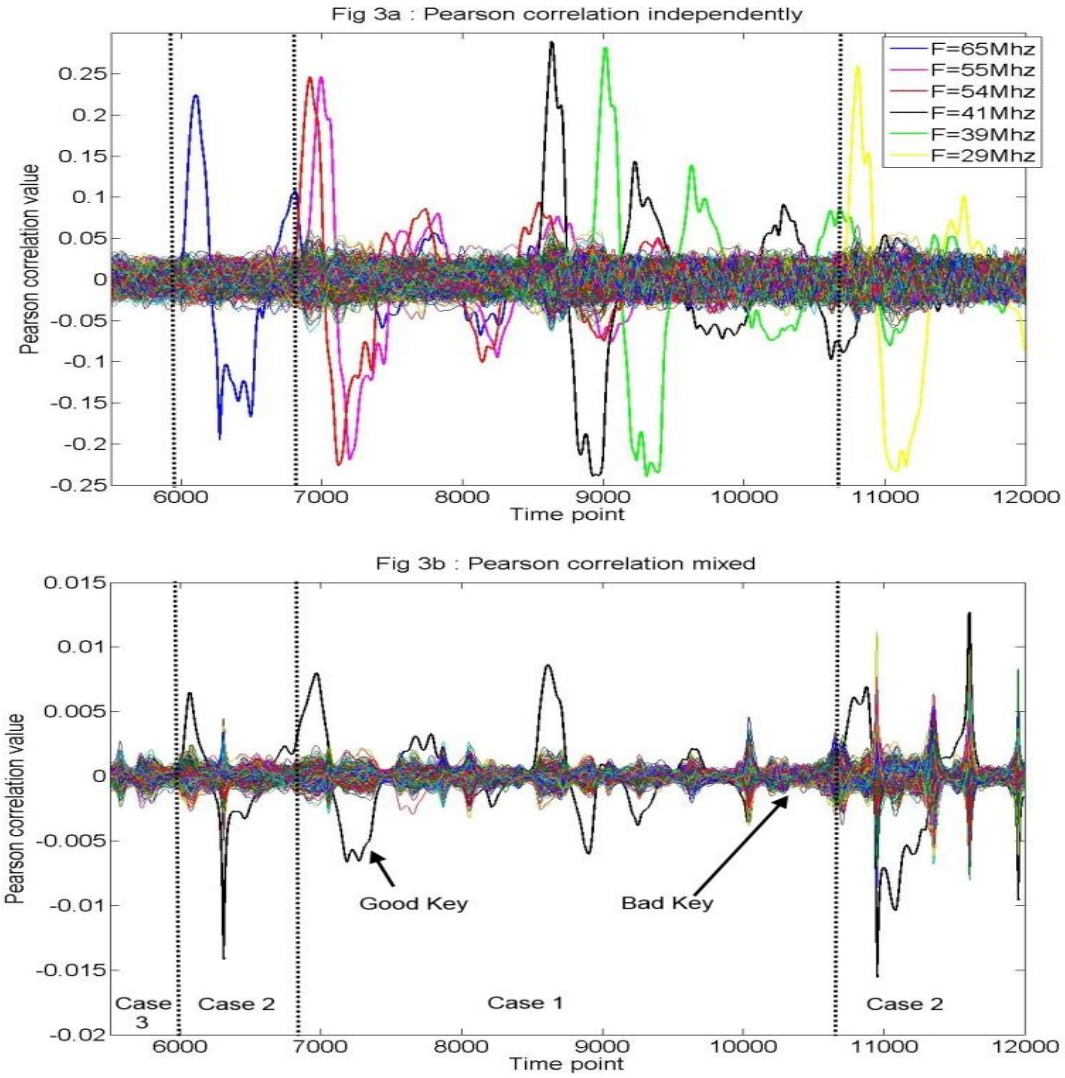
Minor effect against CPA

Effect of changes in Frequency (Random DFS)



Leakage shifted in time by Δt

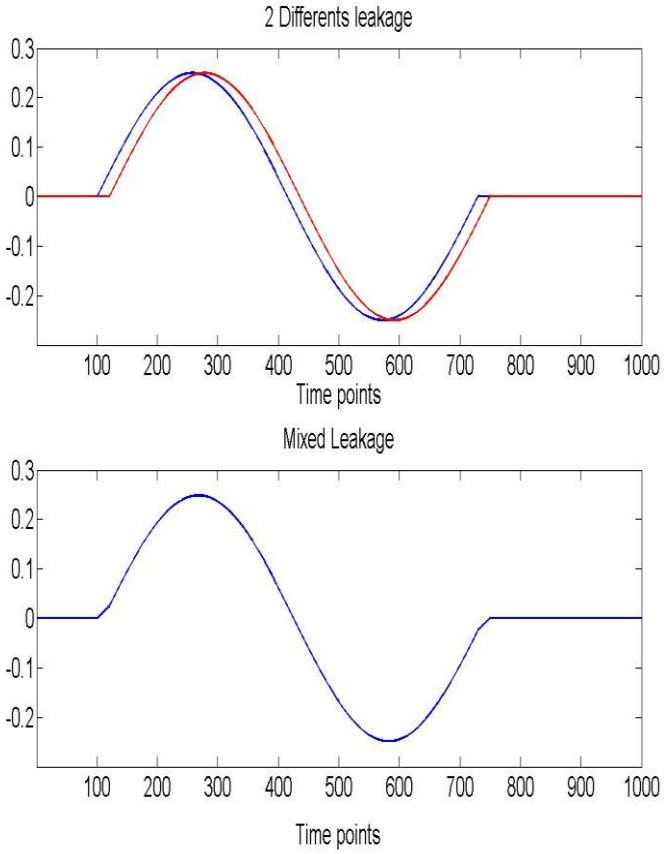
Effect of the Random DVFS



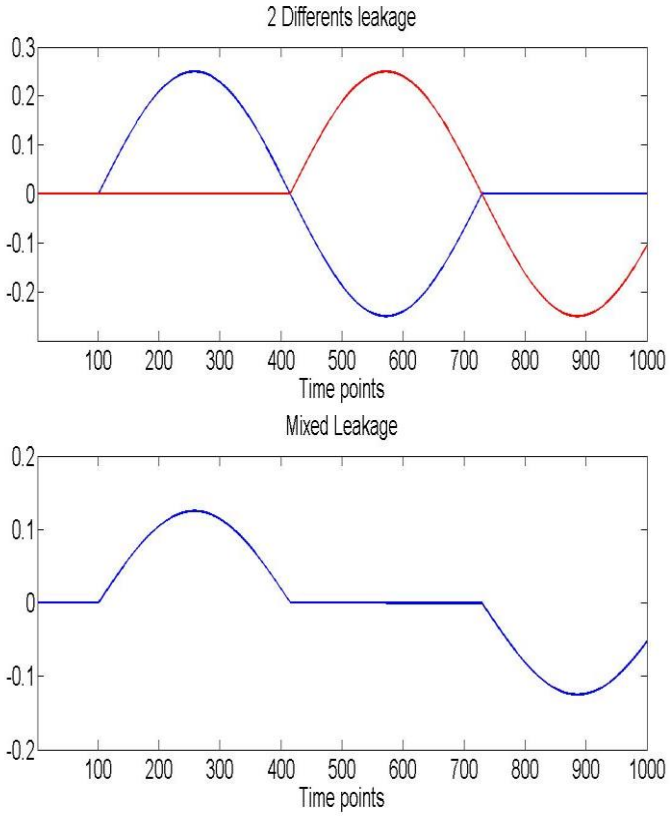
Leakage distributed in time

Effect of the Random DVFS

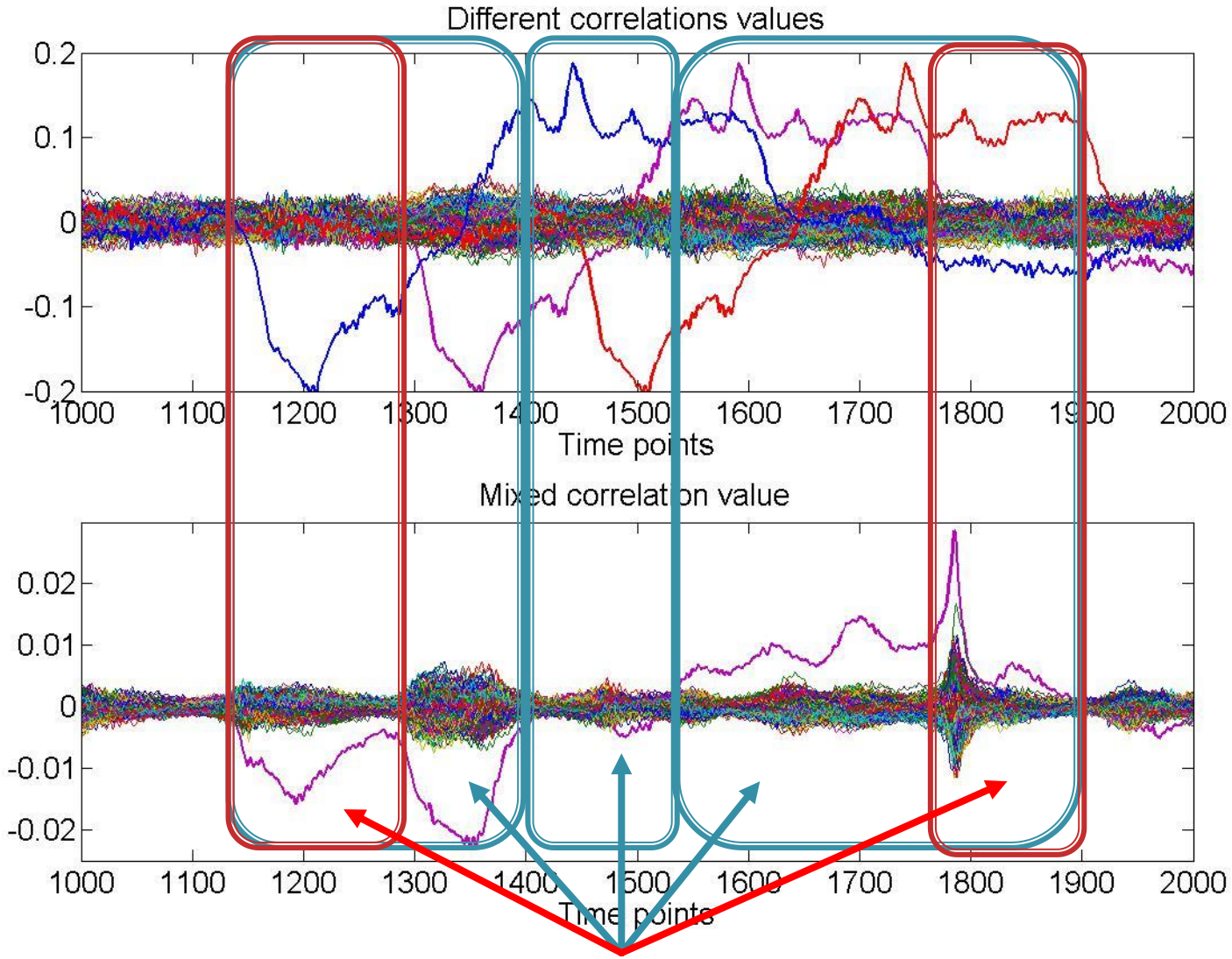
- Best Case



- Worst case



Effect of the Random DVFS

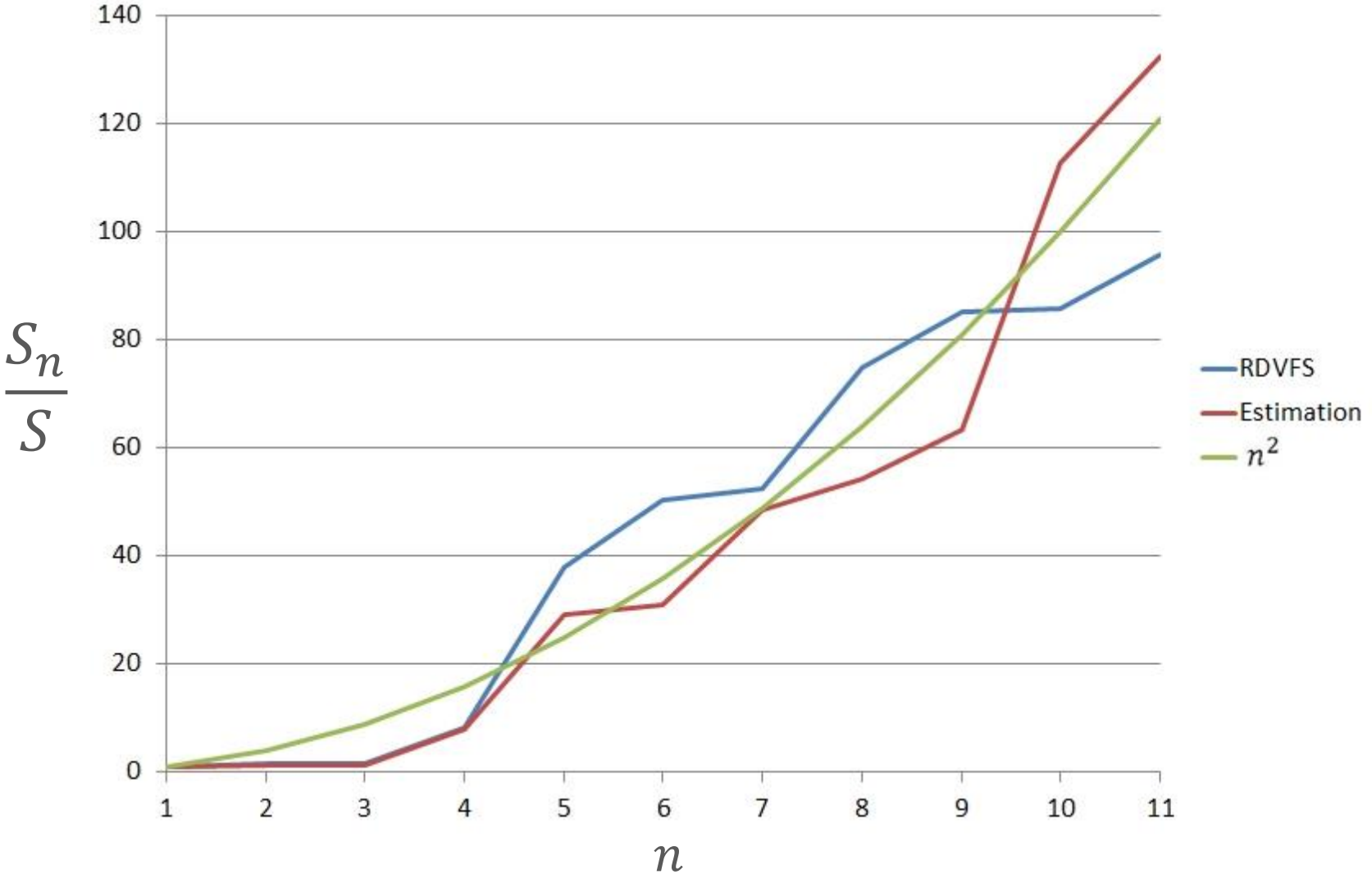


Effect of the Random DVFS (RDVFS)

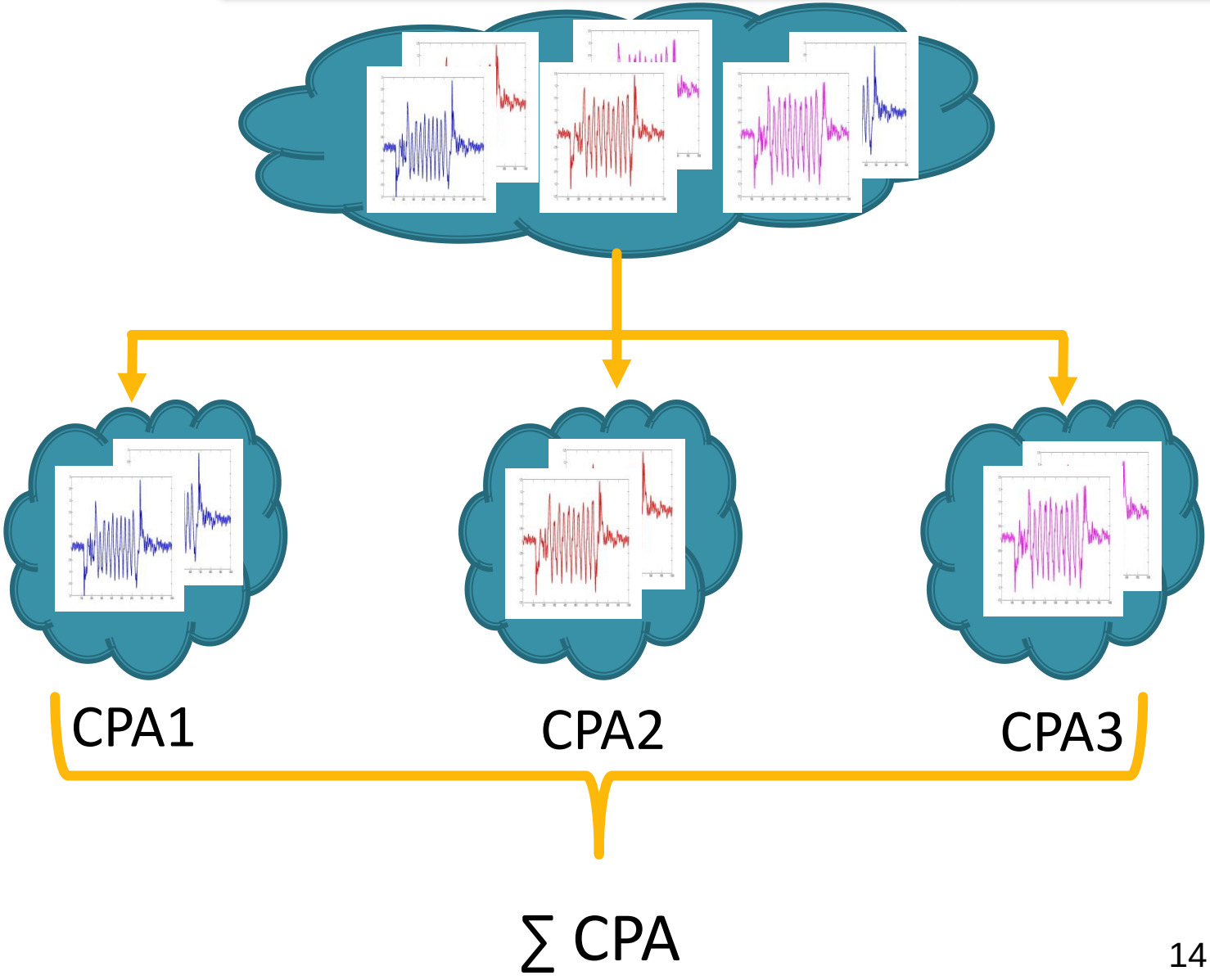
- Theoretical estimation (Mangard)
  - S = Number of curves necessary to obtain the key with fixed V and F values
- Number of curves with Random DVFS (RDVFS)
  - n : Number of couples {V,F}
  - S_n: Number of curves necessary to obtain the key with RDVFS
  - $\frac{S_n}{S}$: Robustness enhancement coefficient
- Theoretical robustness estimation of RDVFS :

$$\frac{S_n}{S} \propto n^2$$

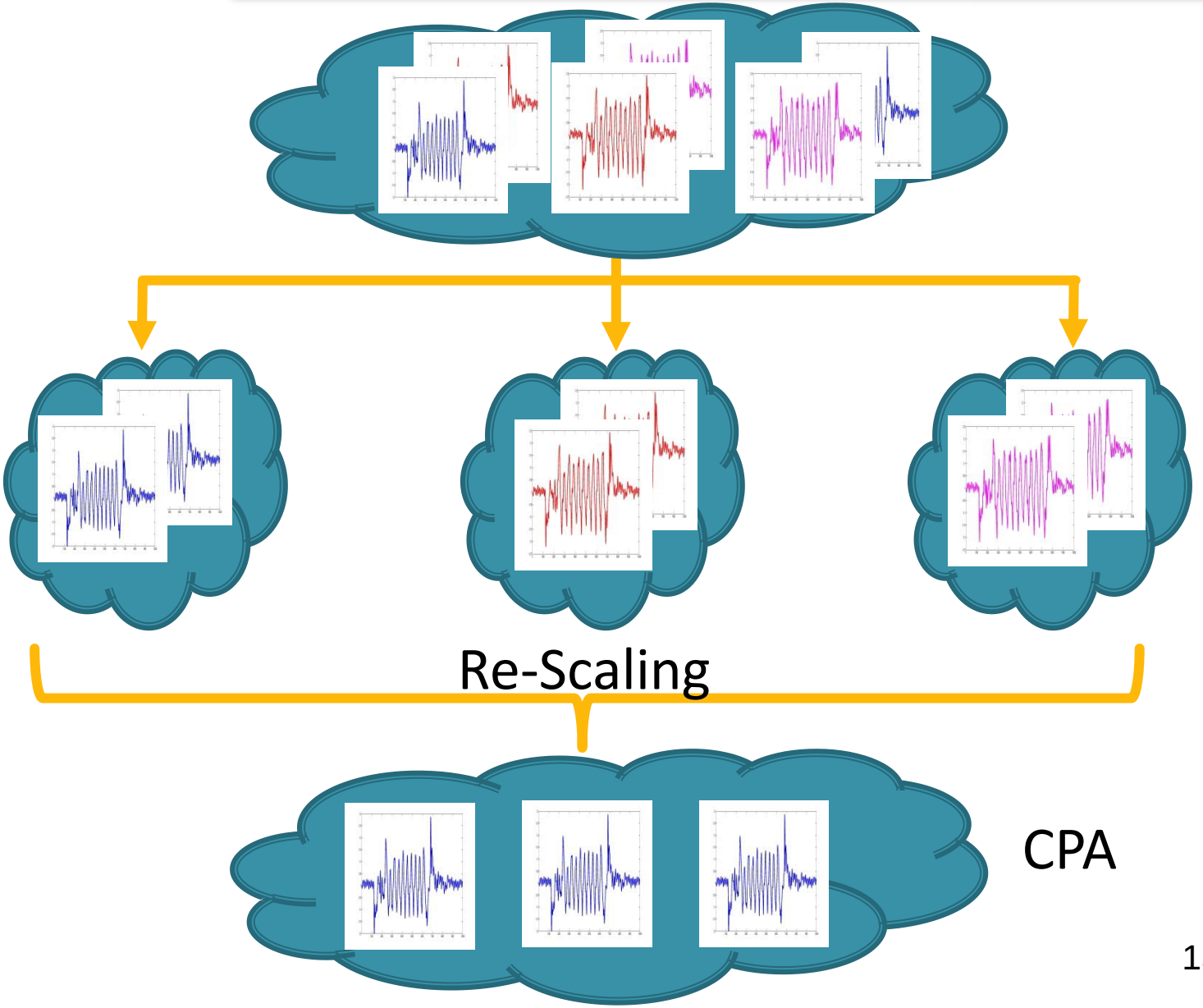
Experimental results



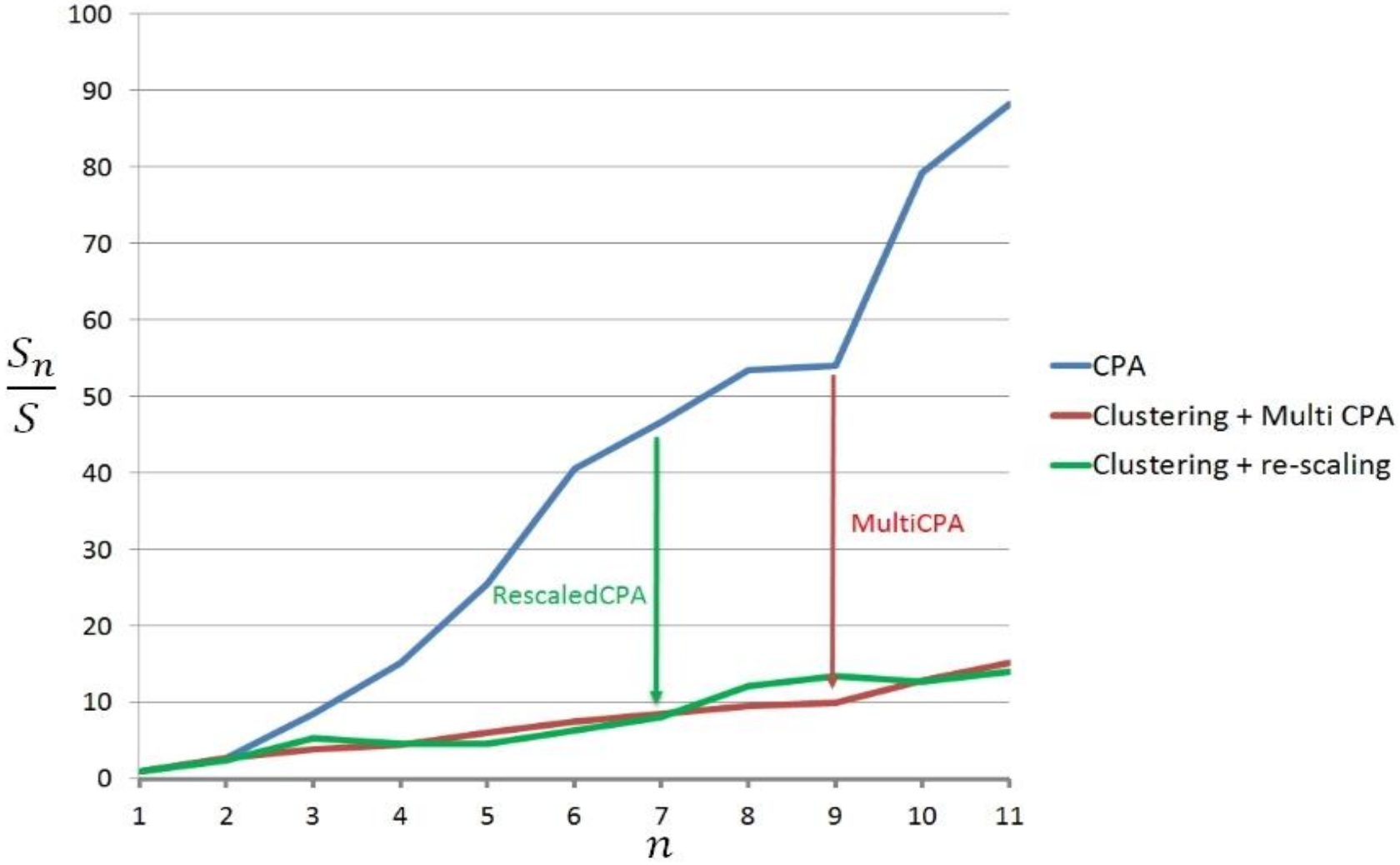
Enhancing CPA efficiency -- Clustering



Enhancing CPA efficiency -- Re-scaling



ENHANCING CPA EFFICIENCY



Conclusion

- Random DVFS increases robustness by n^2
- Robustness can easily be reduced to n by using trace clustering/rescaling
- Possibility of trading performances for security
- Security enhancement is moderated (Linear)

Thank you for your attention

Questions?