Secure Elliptic Curve Implementations : An Analysis of Resistance to Power-Attacks in a DSP Processor

Catherine H. Gebotys[1], Robert J. Gebotys[2]

Department of Electrical and Computer Engineering,

University of Waterloo[1], Wilfrid Laurier University[2], Waterloo, Ontario Canada

cgebotys@optimal.vlsi.uwaterloo.ca

Outline

- *Motivation*
- *Previous Research*
- *Methodology and ISI index*
- *Experimental Results*
- *Conclusions*

Motivation

- *Wireless Communications*
  - *Highly Cost Sensitive*
  - *Low Energy Dissipation*
  - *High Security (data, audio, video)*
- *Secure against Power-Attacks*
  - *Security At all layers*

Previous Research

- *Power / EM / Timing Attacks*
  - *SPA, DPA, [Kocher 96,99]*
  - *SW-DPA [Clavier& 00], IPA [Fahn& 99], n^{th}DPA [Messerges 00],…*
- *DPA extension for ECC [Coron 99]*
- *DSP processors [Dusse 90][Itoh 99]*

Problem Definition

- *Methodology for Design of Secure Embedded Processors*
  - *Secure against power-attacks*
  - *Energy efficient*
  - *Throughput constraints*

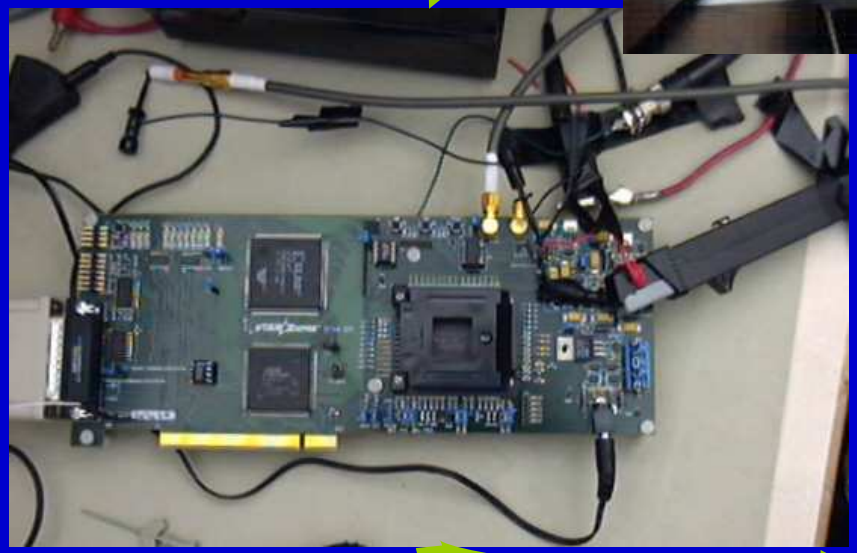
Methodology

- *Point Doubling, Adding*
  - *Timing and Power Traces identical through adding redundant operations*
- *Point Multiplication*
  - *Timing and Power Traces identical through looping and switching*

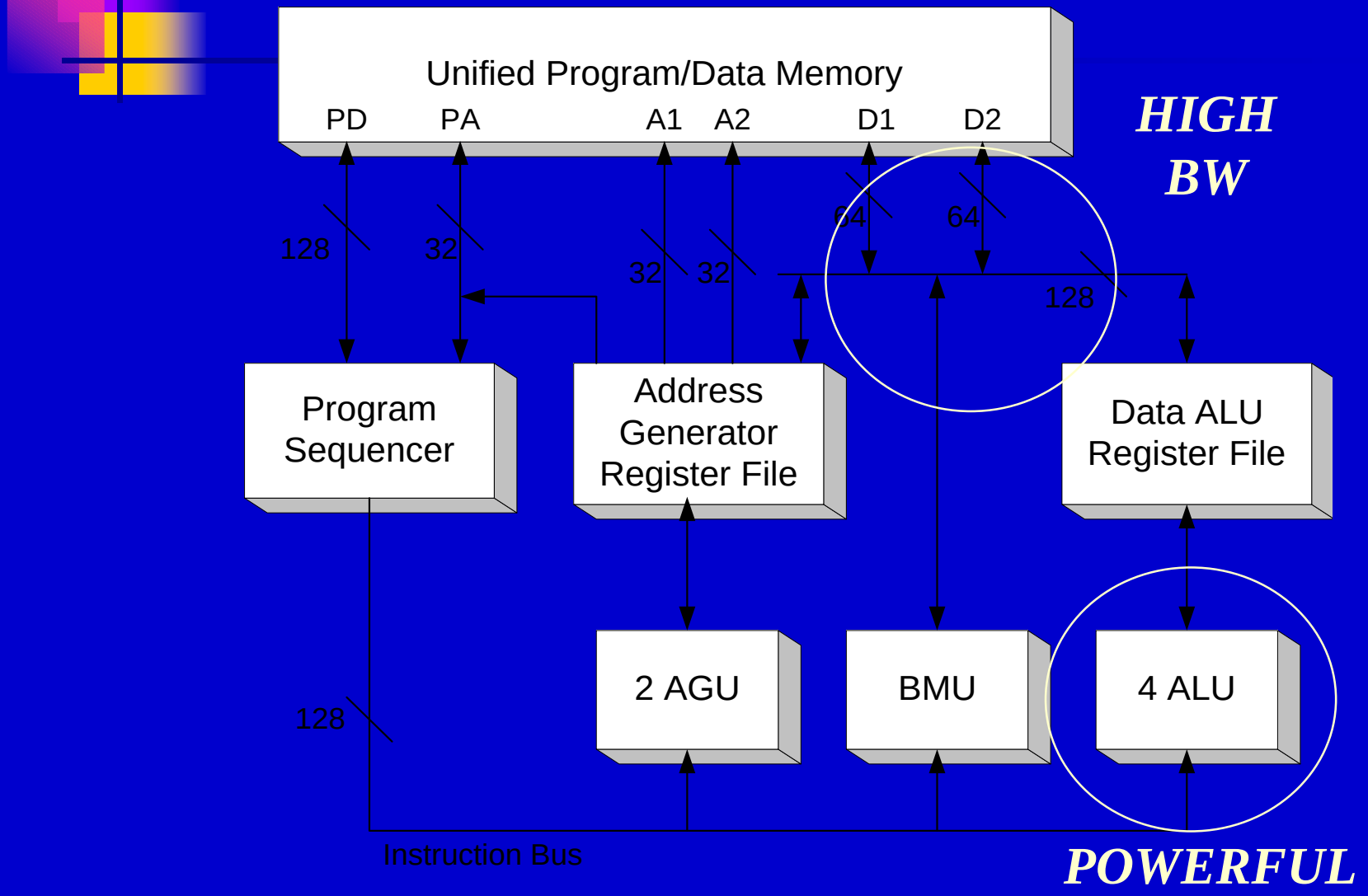
Experimental Results

- *Elliptic Curve Cryptography*
  - *Weierstrass (projective coordinates)*
  - *Jacobi form of curve*
  - *192-bit prime fields*
- *DSP processor core at 100MHz*

Research Setup

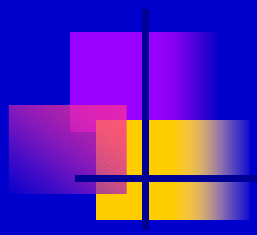


Star*core Architecture



Cycle Counts

Point:	***Cycles***
Double	***3,177***
Sum	***5,554***
Field:	
Multiplication	***330***
Squaring	***213***
Addition	***33***



DOUBLE

b1 = y ^2
e1 = z ^2
b2 = b1 * b1
b = b2<<3
__z2=y2 * x2
z31 = y * z
e2 = x - e1
e3 = x + e1
e = e2 * e3
z12 = z31<<1
c1 = e<<1
c = c1 + e
f1 = b1<<2
a = f1 * x
f3 = a<<1
d1 = c * c
x12 = d1 - f3
y31 = a - x3
y32 = y31 * c
y12 = y32 - b

SUM 1

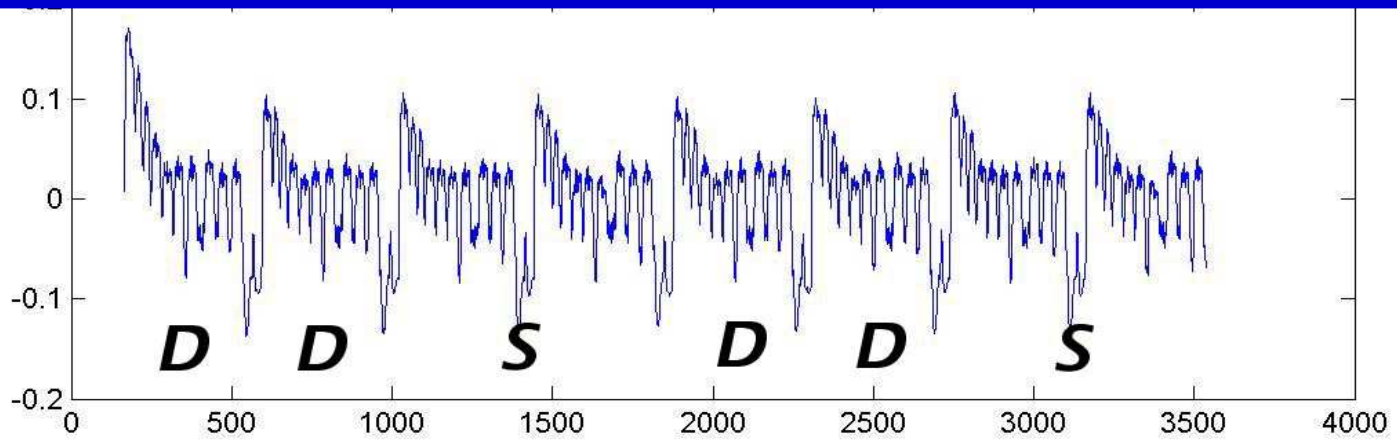
z2s = z2 ^2
z1s = z1 ^2
z2c = z2s * z2
__al=y2<<3
f = z1s * x2
g = z2s * x1
___th=x1-z1s
___ga=x1+z1s
z1c = z1s * z1
___om=g<<1
___ga=z1c<<1
th = f + g
___al=z2s<<2
ga = z1 * z2
___la=ga<<1
i = y1 * z2c
___al=i-la
h = f - g
om = y2 * z1c
j = om - i

SUM 2

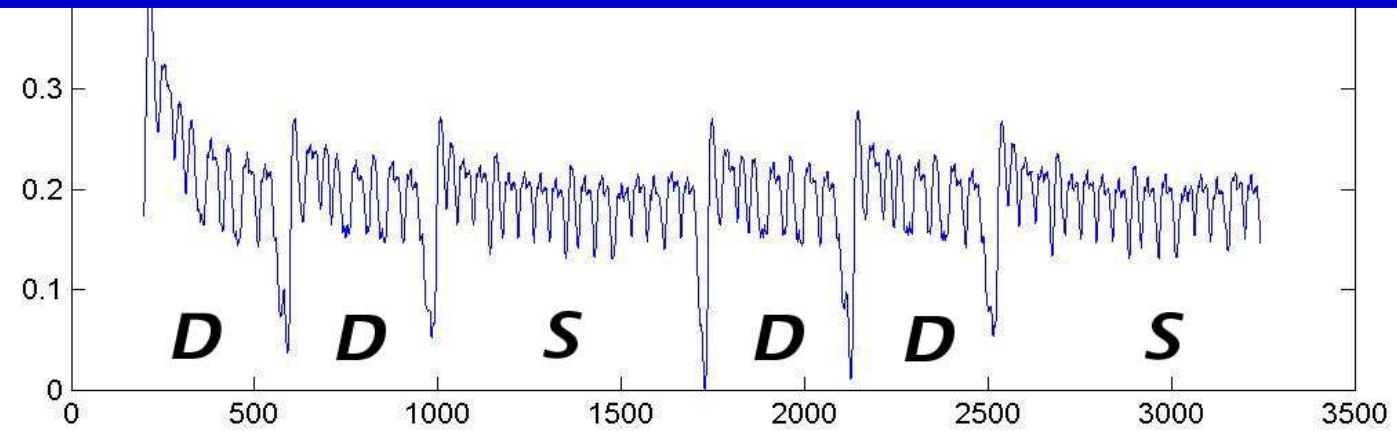
hs = h ^2
om = j ^2
al = th * hs
__th=y2<<3
la = h * hs
th = la * i
x3 = om - al
___be=al + om
z3 = ga * h
___al=hs<<1
___be=z3<<1
___om=be+z3
___ga=hs<<2
la = hs * g
___al=la<<1
___be=om*om
om = la –x3
___ga=om-al
al = om * j
y3 = al - th

Power Traces

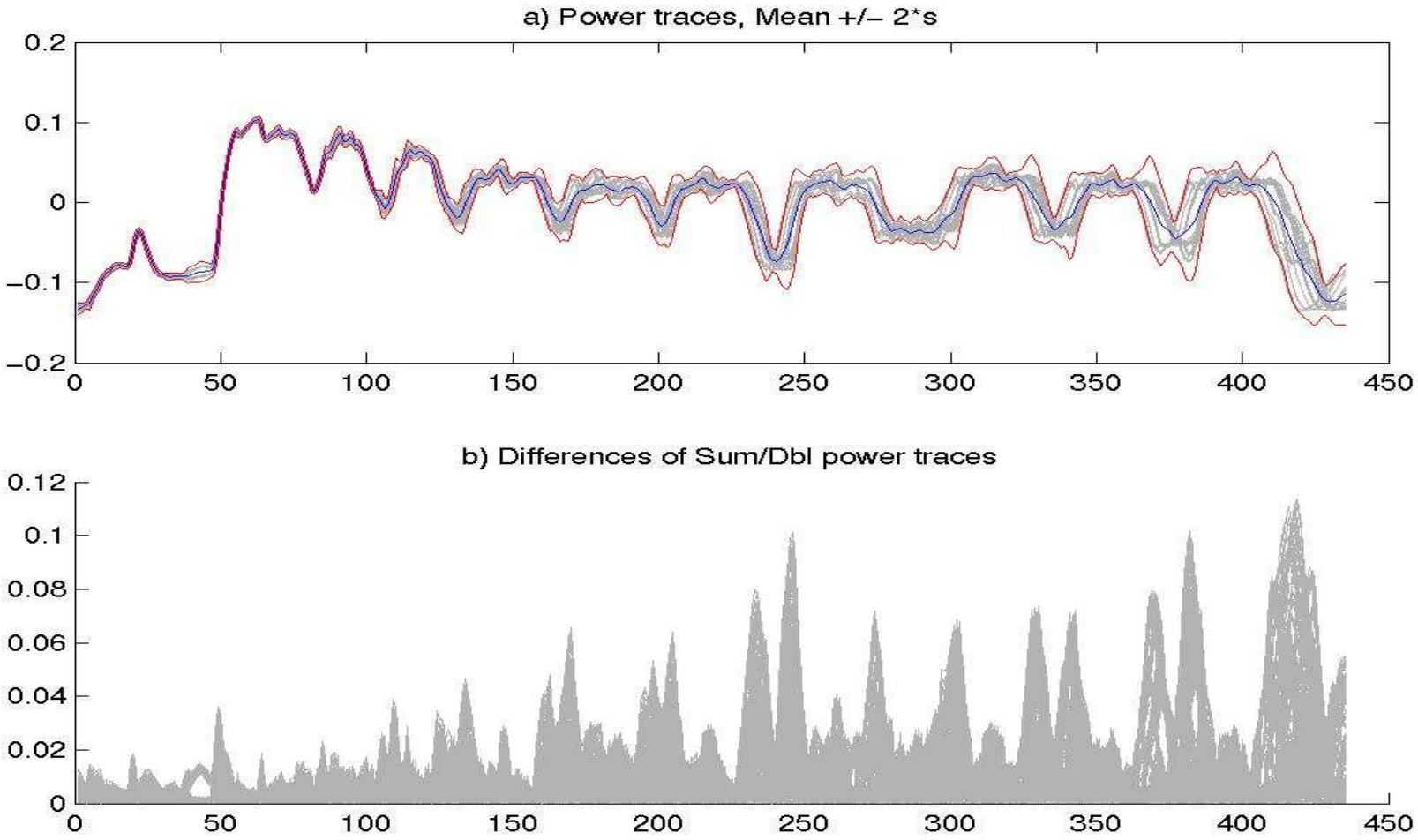
PA-resistant ECC Code



Original ECC Code



Power Traces – timing shifts

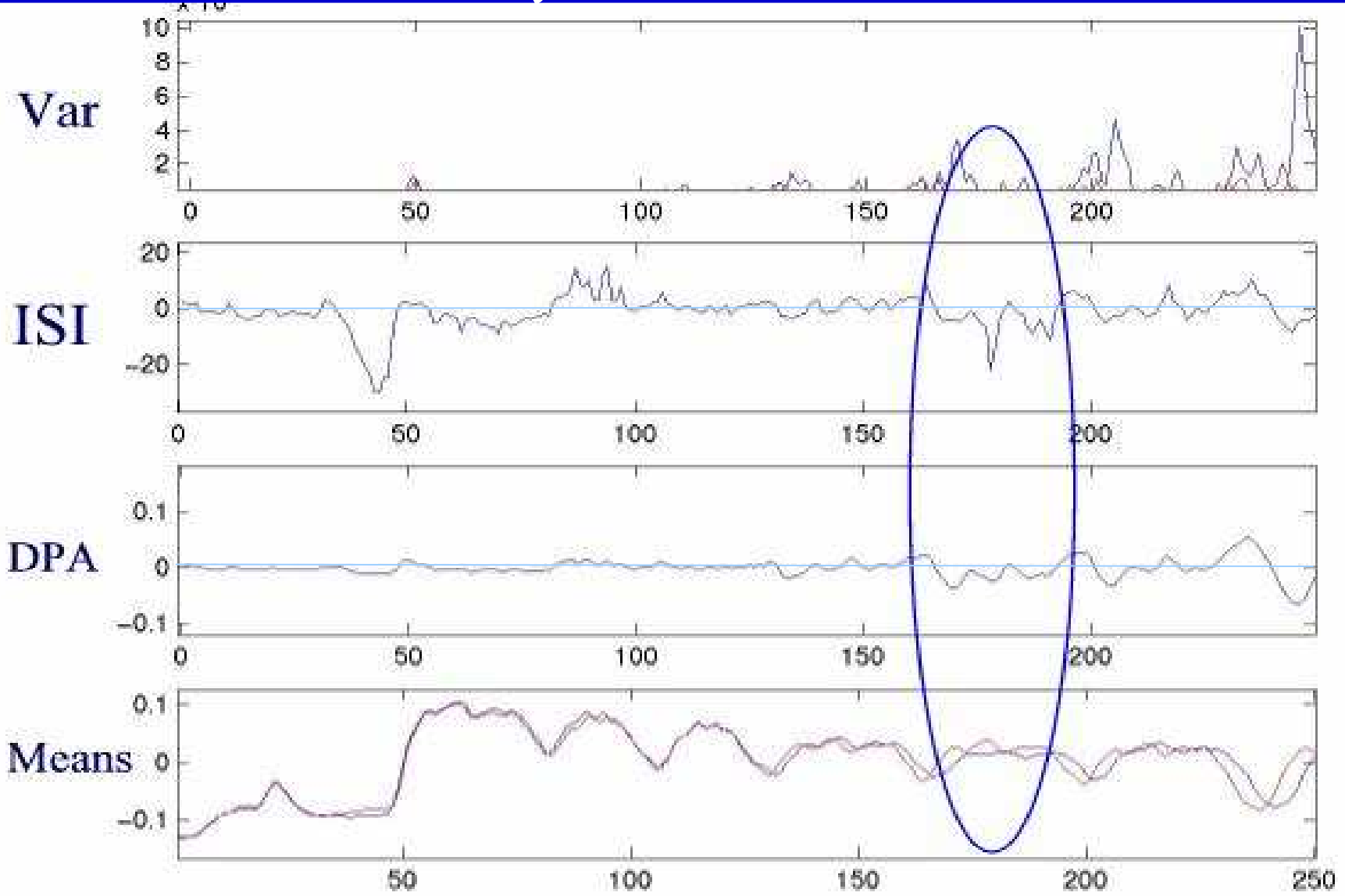


Implementation Security Index

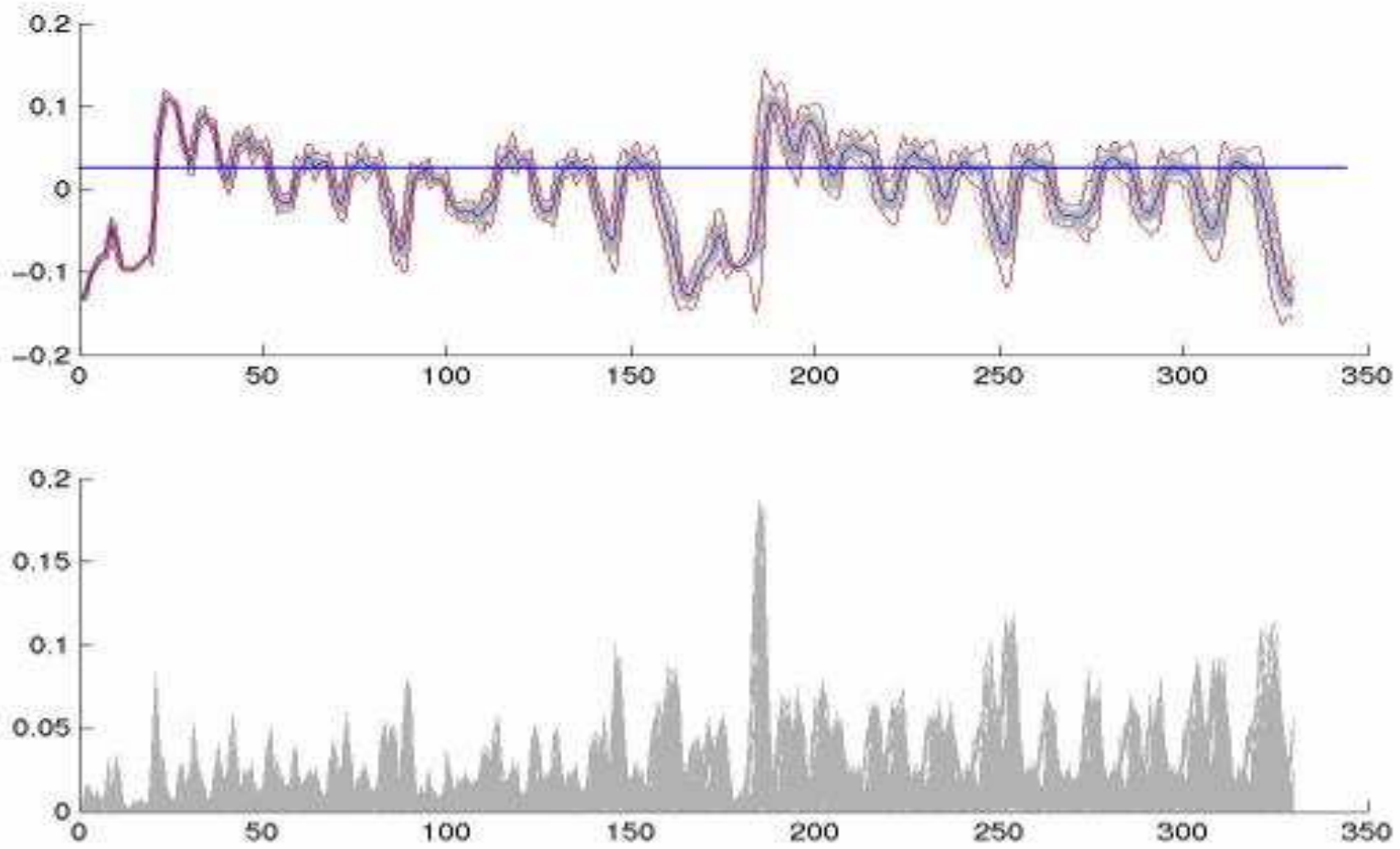
$$ISI_{1,2}(t) = \left(\frac{(\bar{x}_1(t) - \bar{x}_2(t))}{\sqrt{\frac{(s_1(t))^2}{n_1} + \frac{(s_2(t))^2}{n_2}}} \right)^{-1} \quad (1)$$

Incorporates Variance into Difference of Means

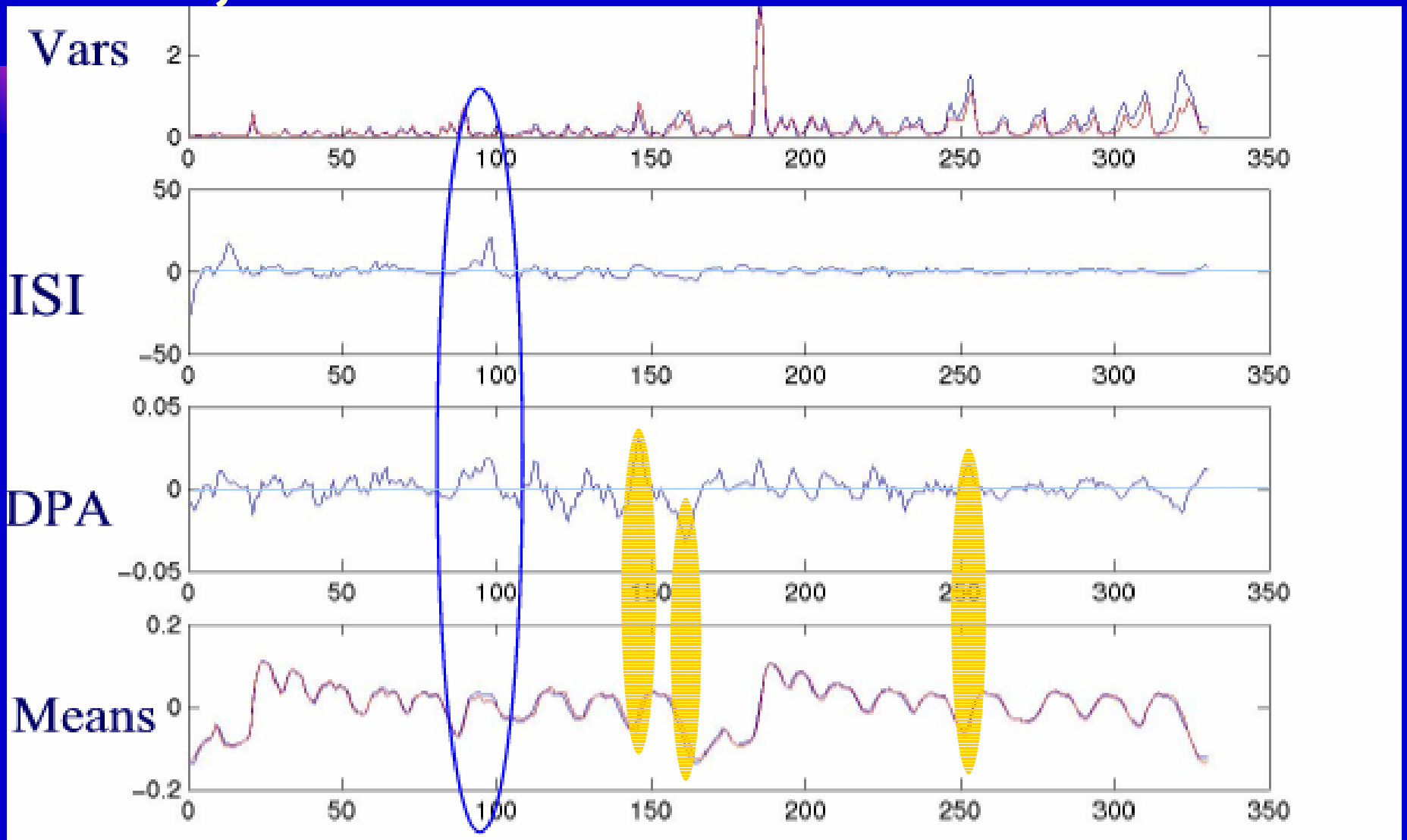
$ISI_{s,D}(t)^{-1}$ vs DPA



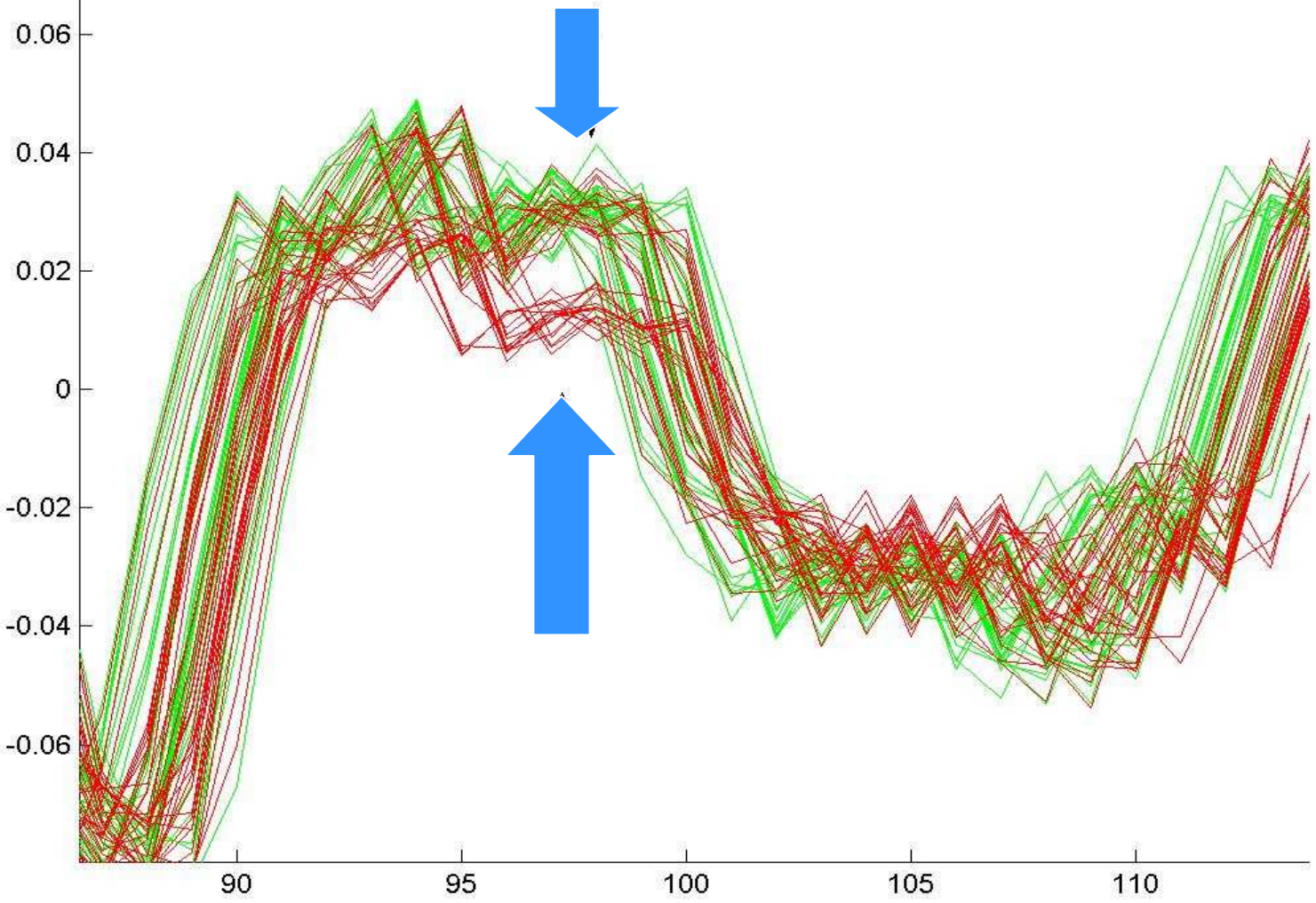
Sum–Double Power Traces



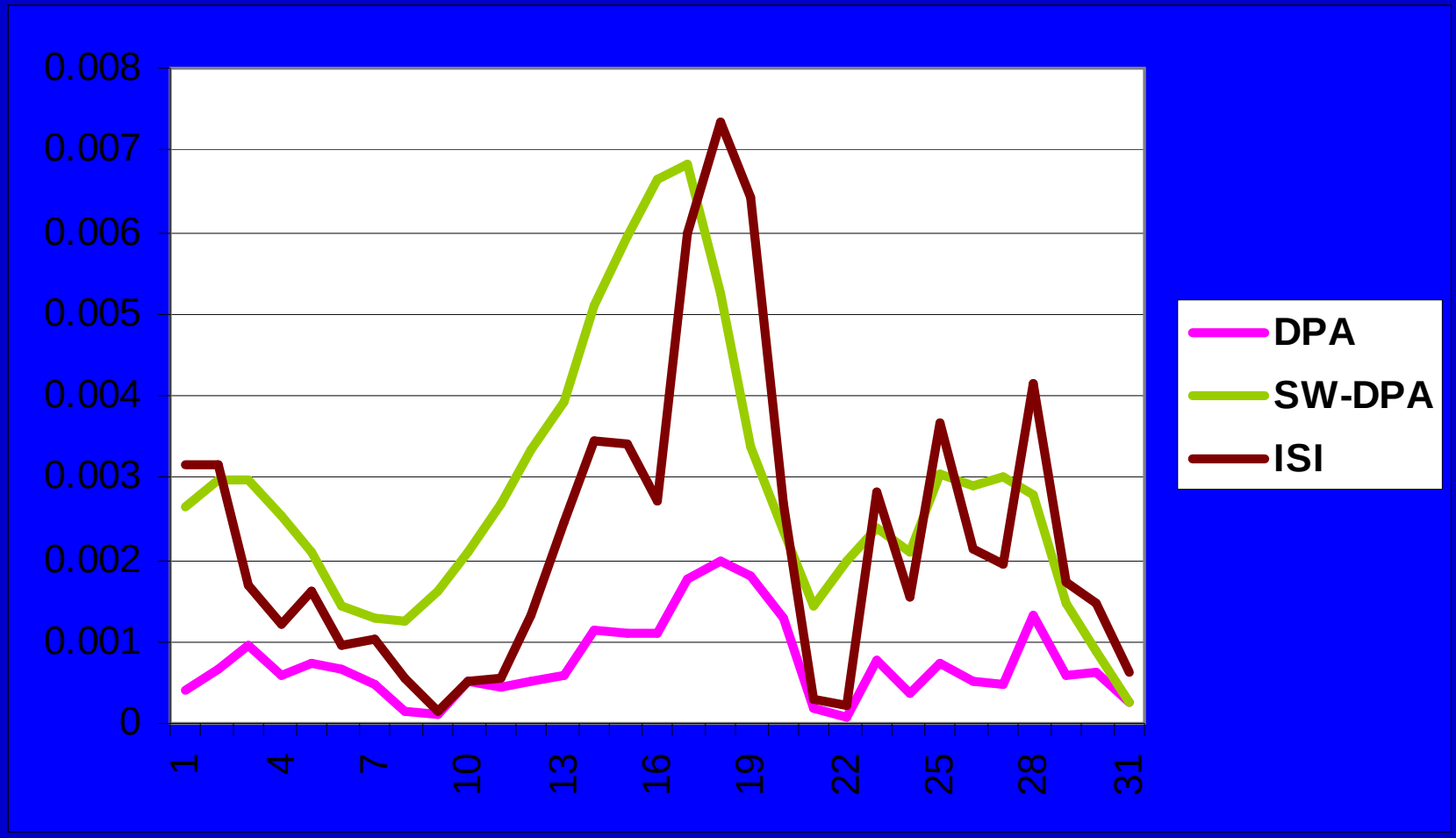
$ISI_{DS,SD}(t)^{-1}$ vs DPA



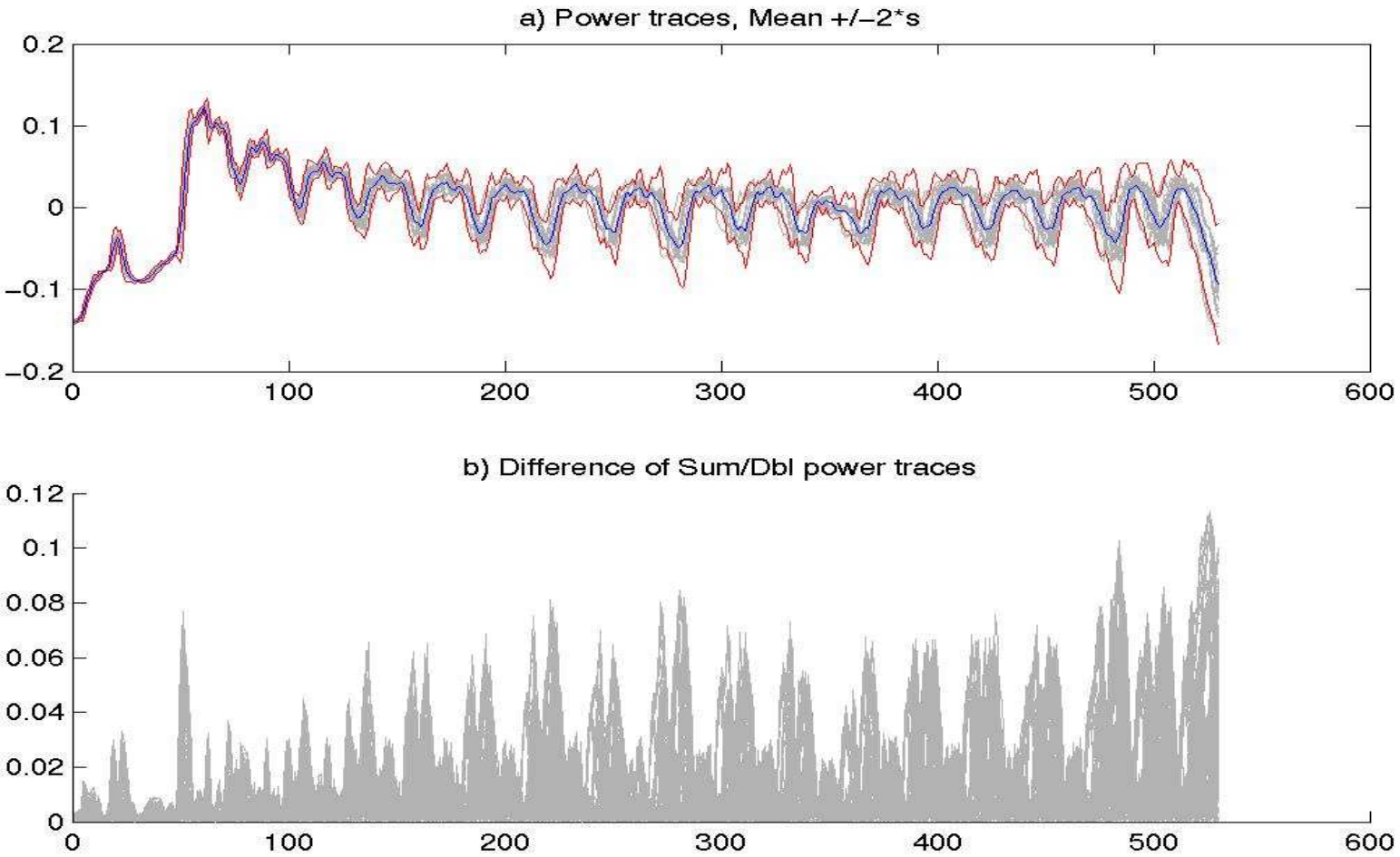
Memory Stalls : Power



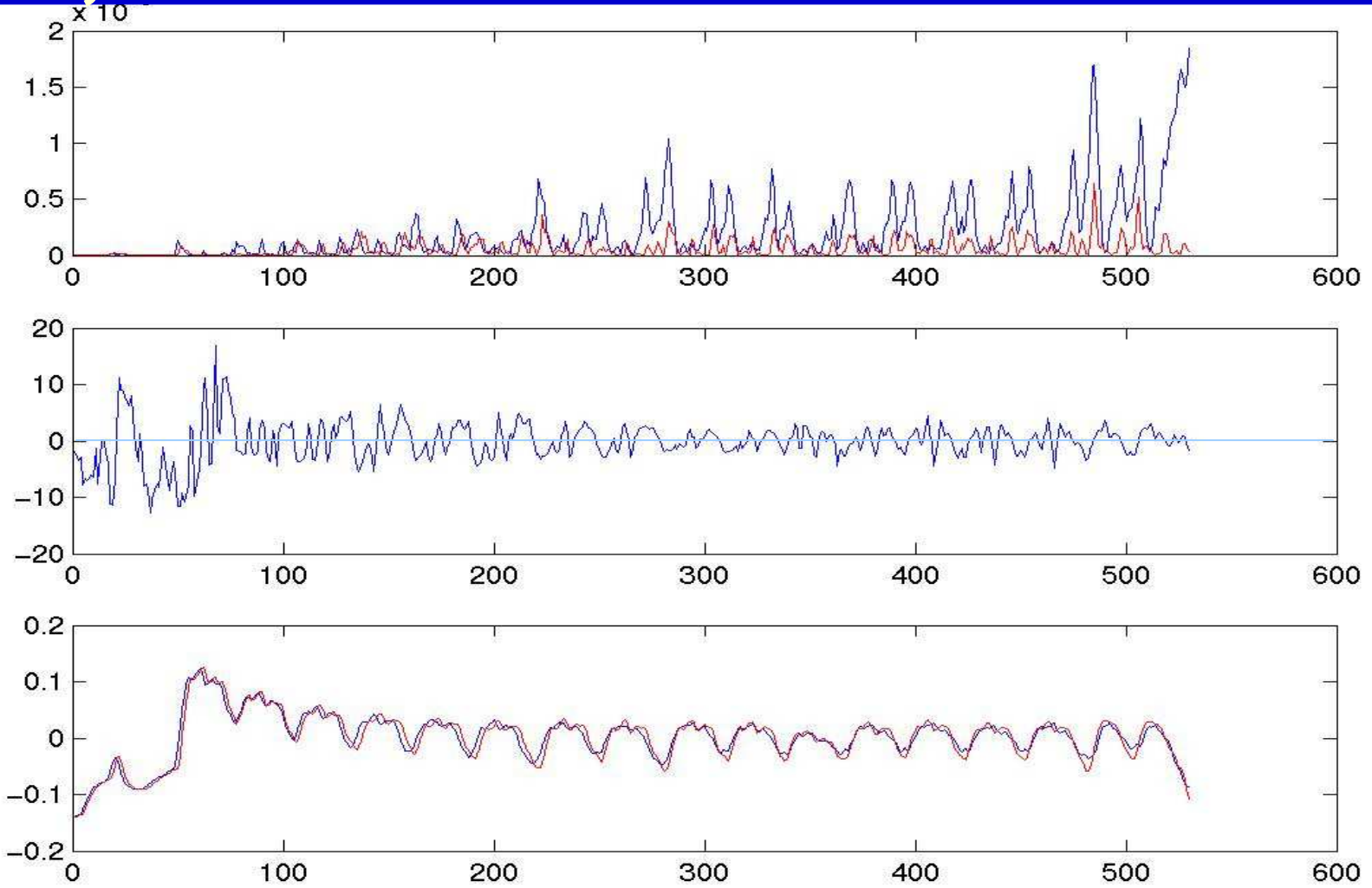
Comparison to SW-DPA



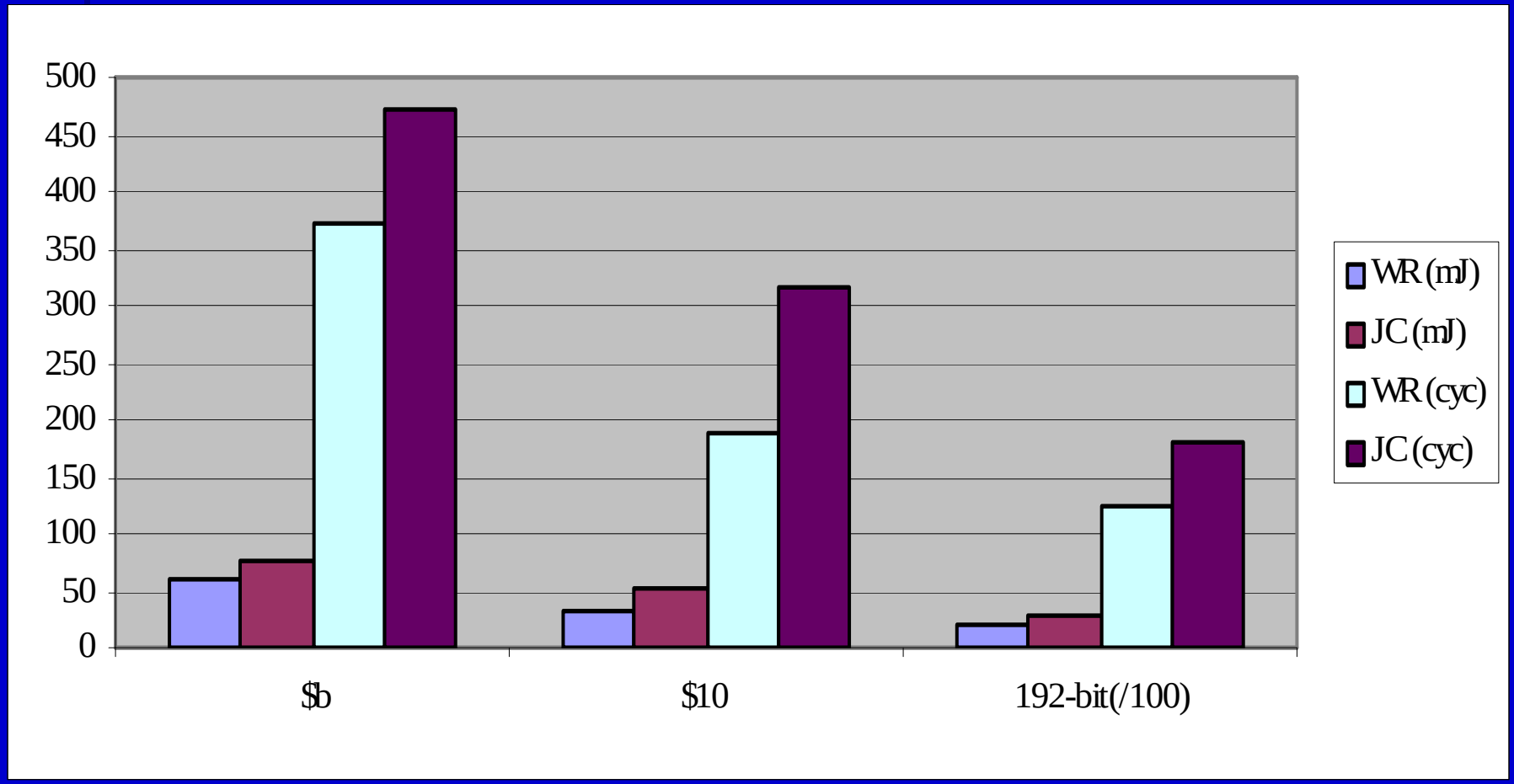
Jacobi Form of Curve



$ISI_{S,D}(t)^{-1}$: Jacobi Curve



Energy – Performance Comparison



Conclusions

- *Security against Power-Attack*
  - *ISI Metric for software development*
- *ISI : Variances plus Difference of Means*
  - *Timing Shifts , Parallelism*
  - *Complex Processor Cores*