EM Analysis of Rijndael and ECC on a Wireless Java-based PDA

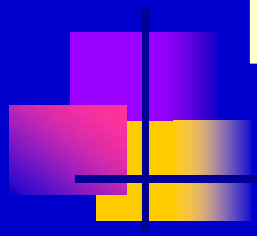
C.Gebotys, S.Ho, C.C.Tiu

Dept of Electrical and Computer Engineering,

University of Waterloo,

Waterloo, Ontario Canada

cgebotys@uwaterloo.ca



Motivation

- *Security in Embedded Systems*
  - *Smartcards, PDAs, Cellphones, etc*
  - *VPN, line accelerators, cars,…*
- *Countermeasures*
  - *Suitable for constraints of embedded system*

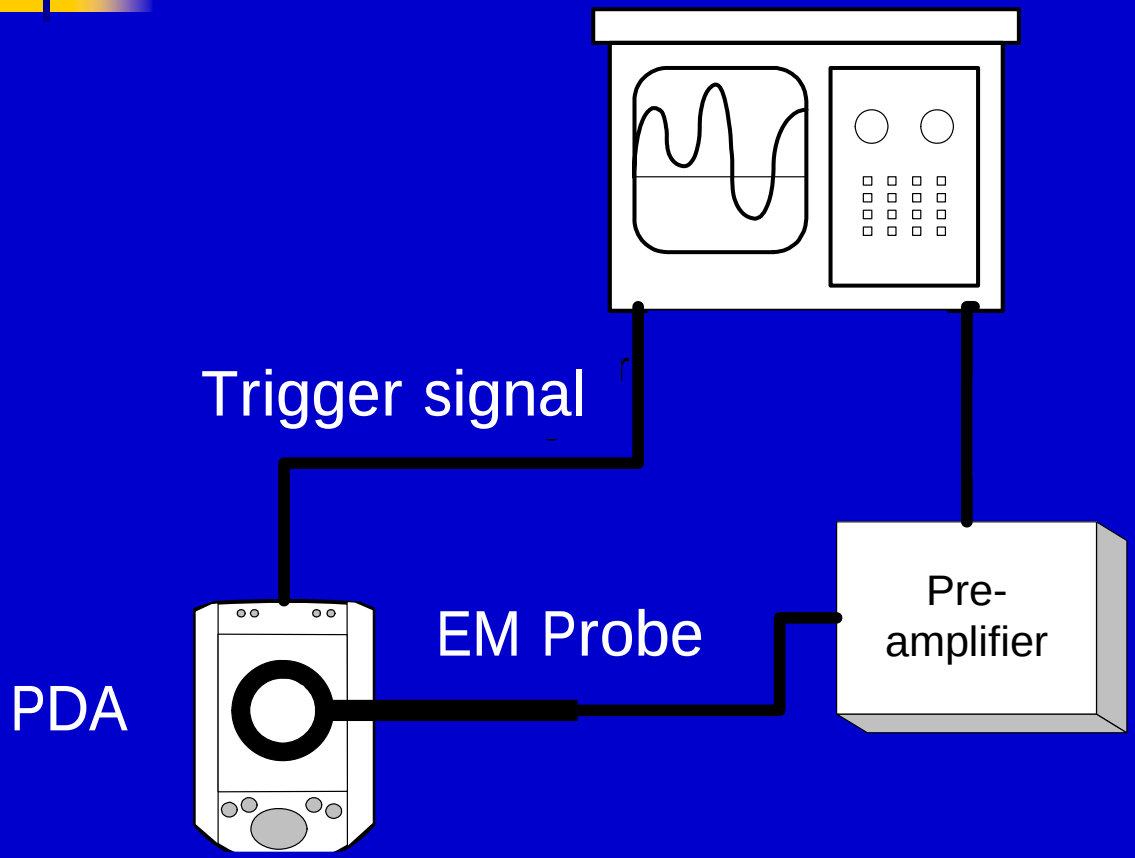
Previous Research

- *Power & EM Attacks*
  - DPA *(Kocher 96,99), (Clavier& 00), (Fahn& 99), (Messerges 00),* DEMA (Gandolfi& 01), (Agrawal& 02) (Carlier& 04),…
- *Countermeasures*
  - *1.9 times latency, # memory accesses large, or large tables stored*

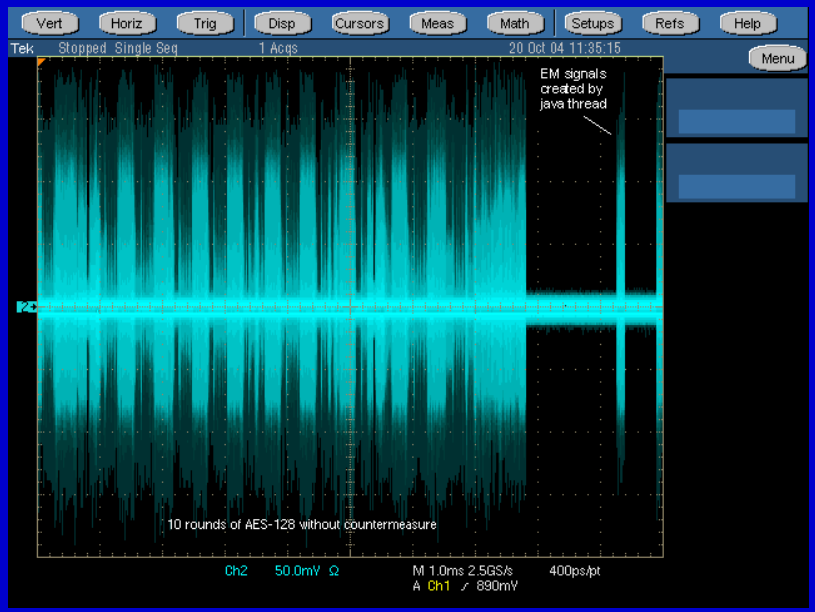
Problem Definition

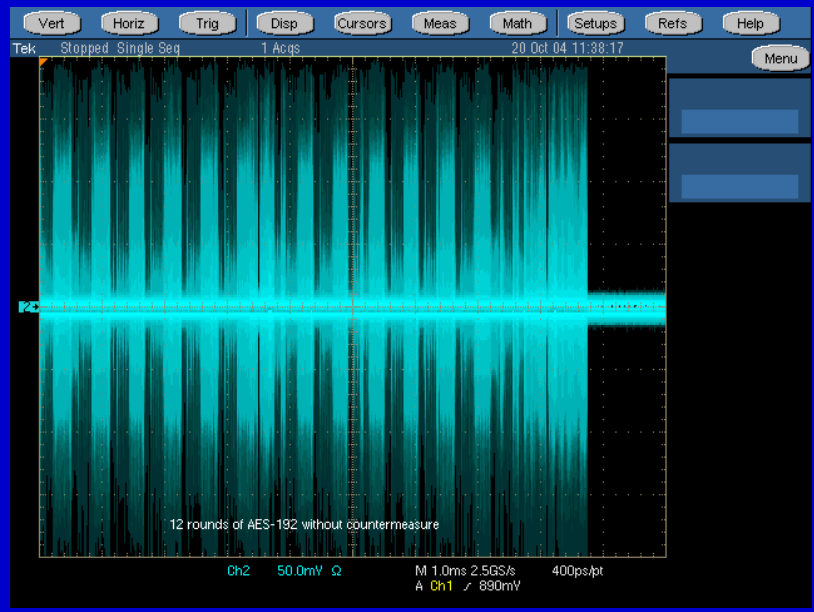
- *PDA Side Channel Attack*
  - *EM analysis*
- *Low Energy Countermeasure Design for PDAs*
  - *Resistance from EM-attacks*

Experimental Setup : PDA

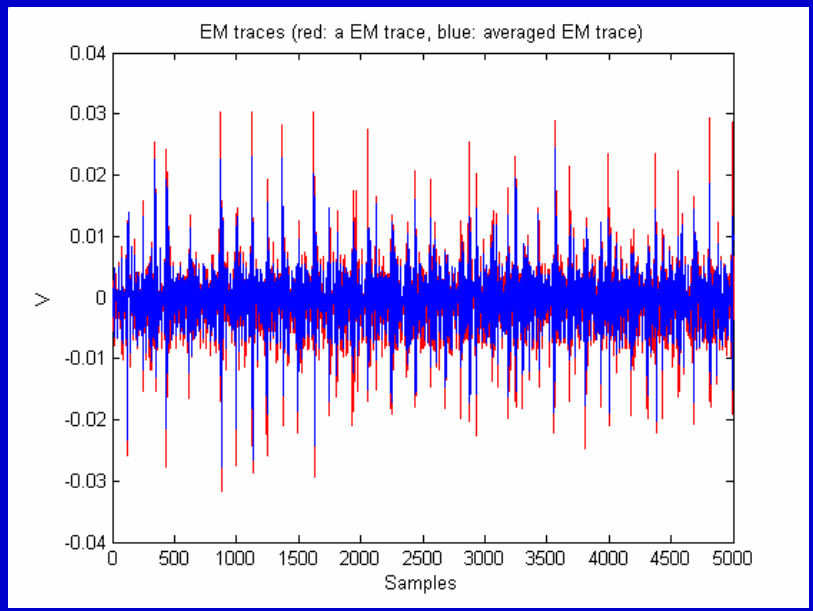


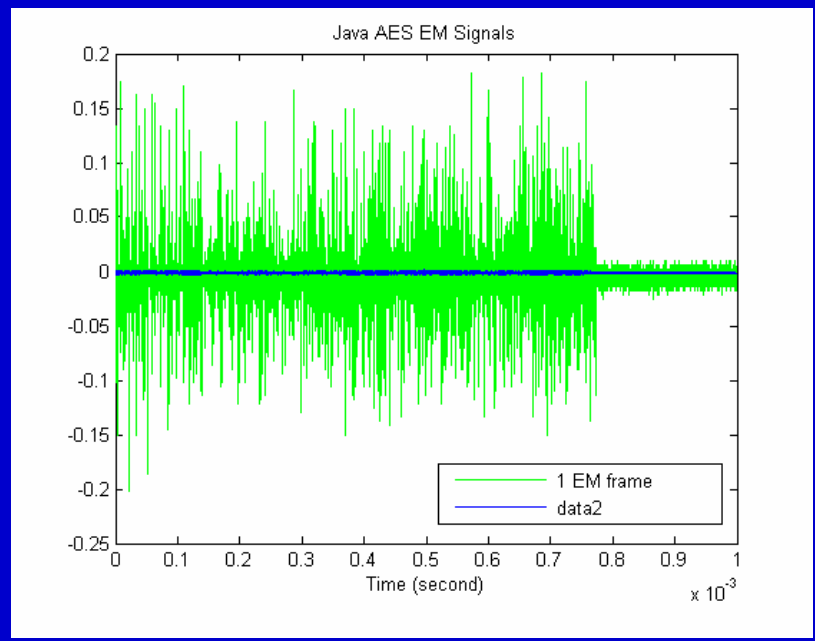
EM of Rijndael Rounds on PDA



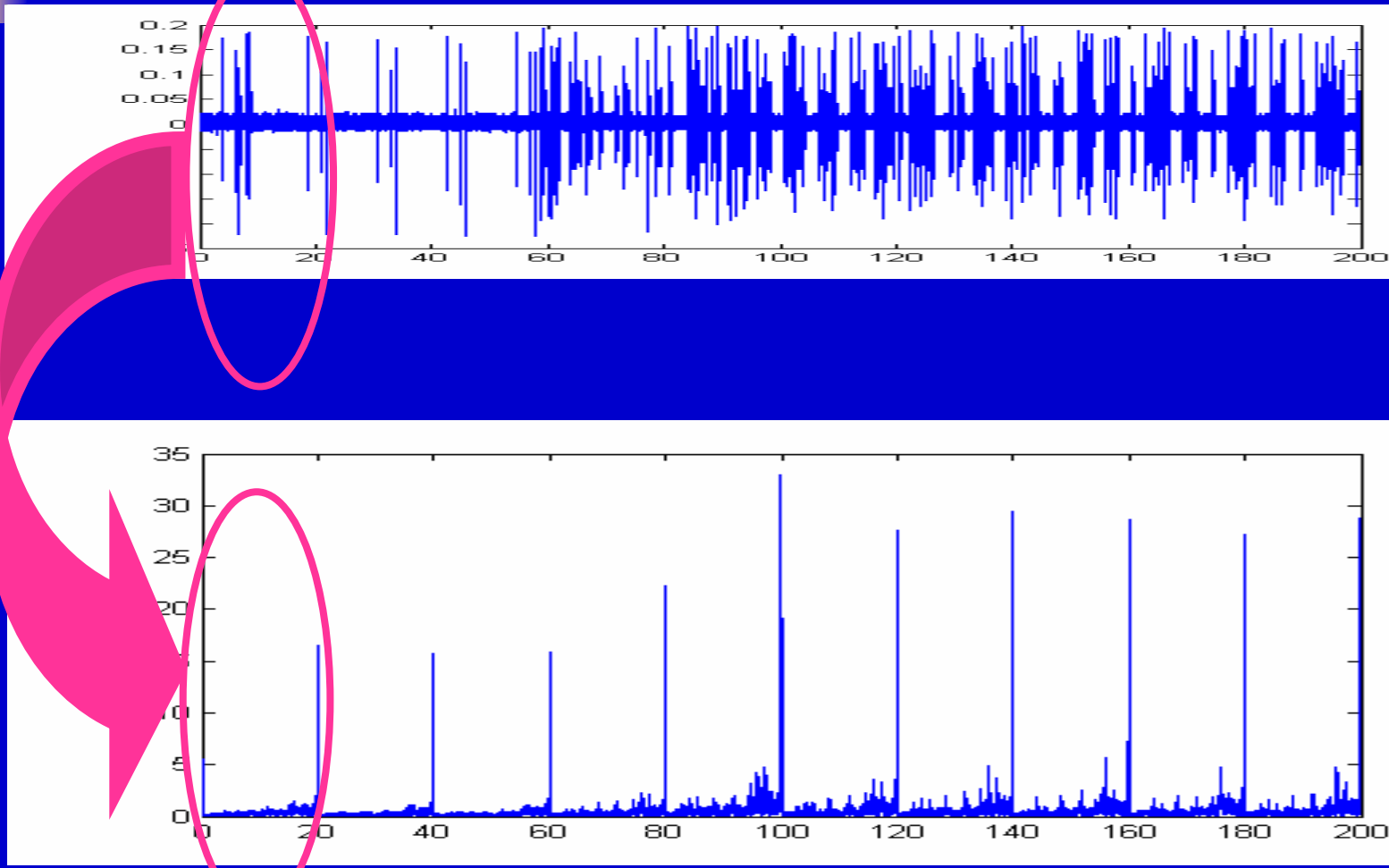


Averaged EM Traces on ARM7 and PDA

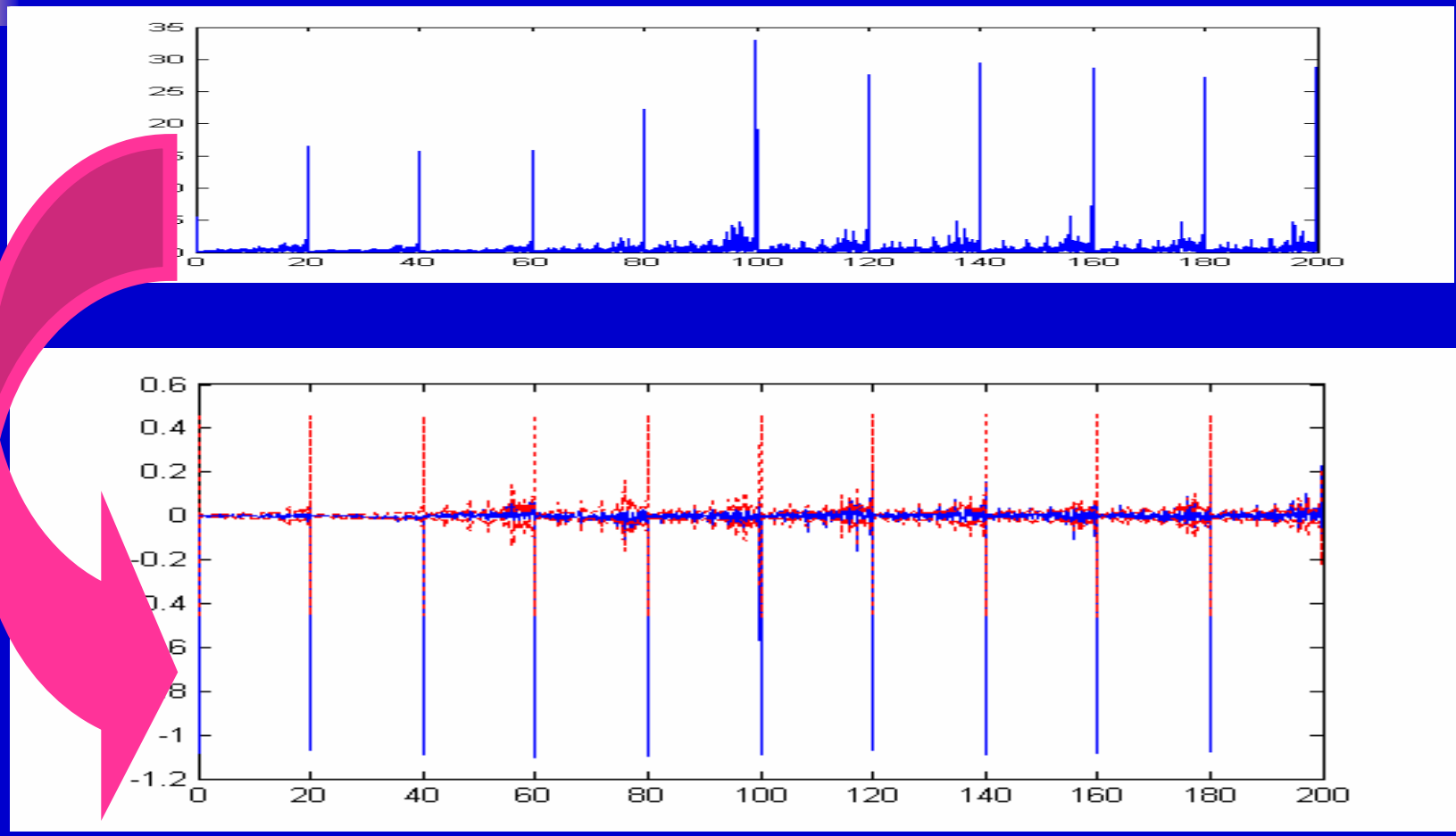




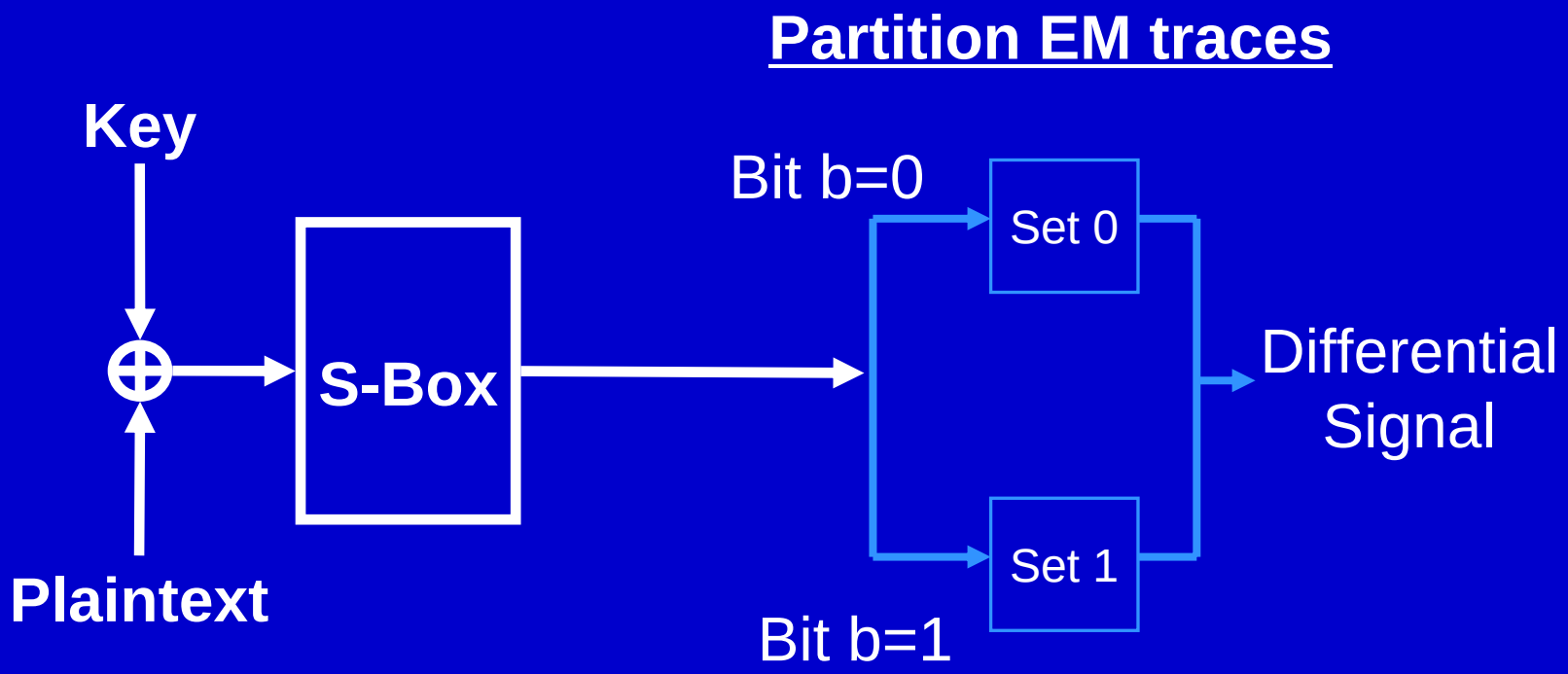
Frequency-based Differential Analysis: Spectrogram



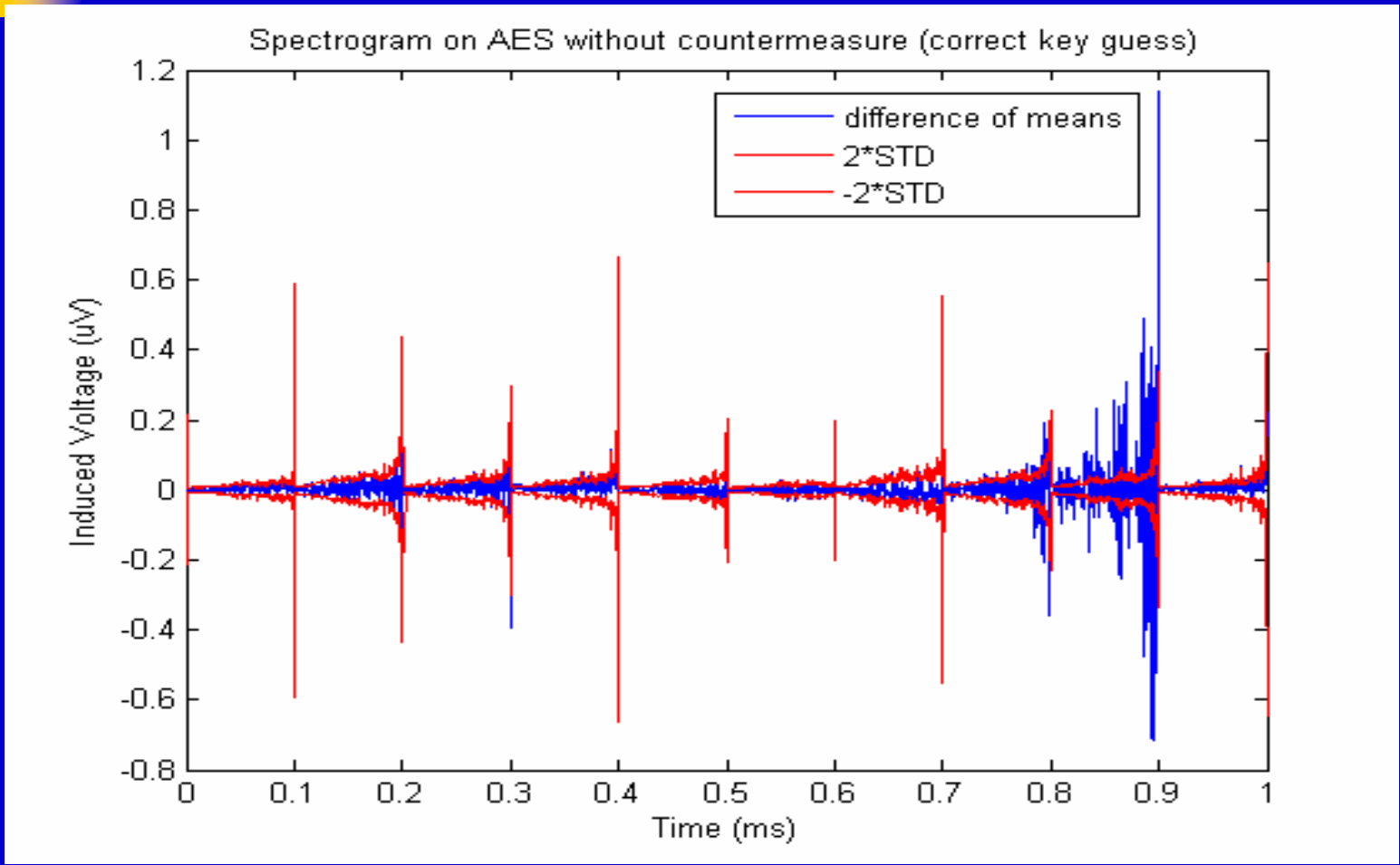
Difference of Means of Spectrograms



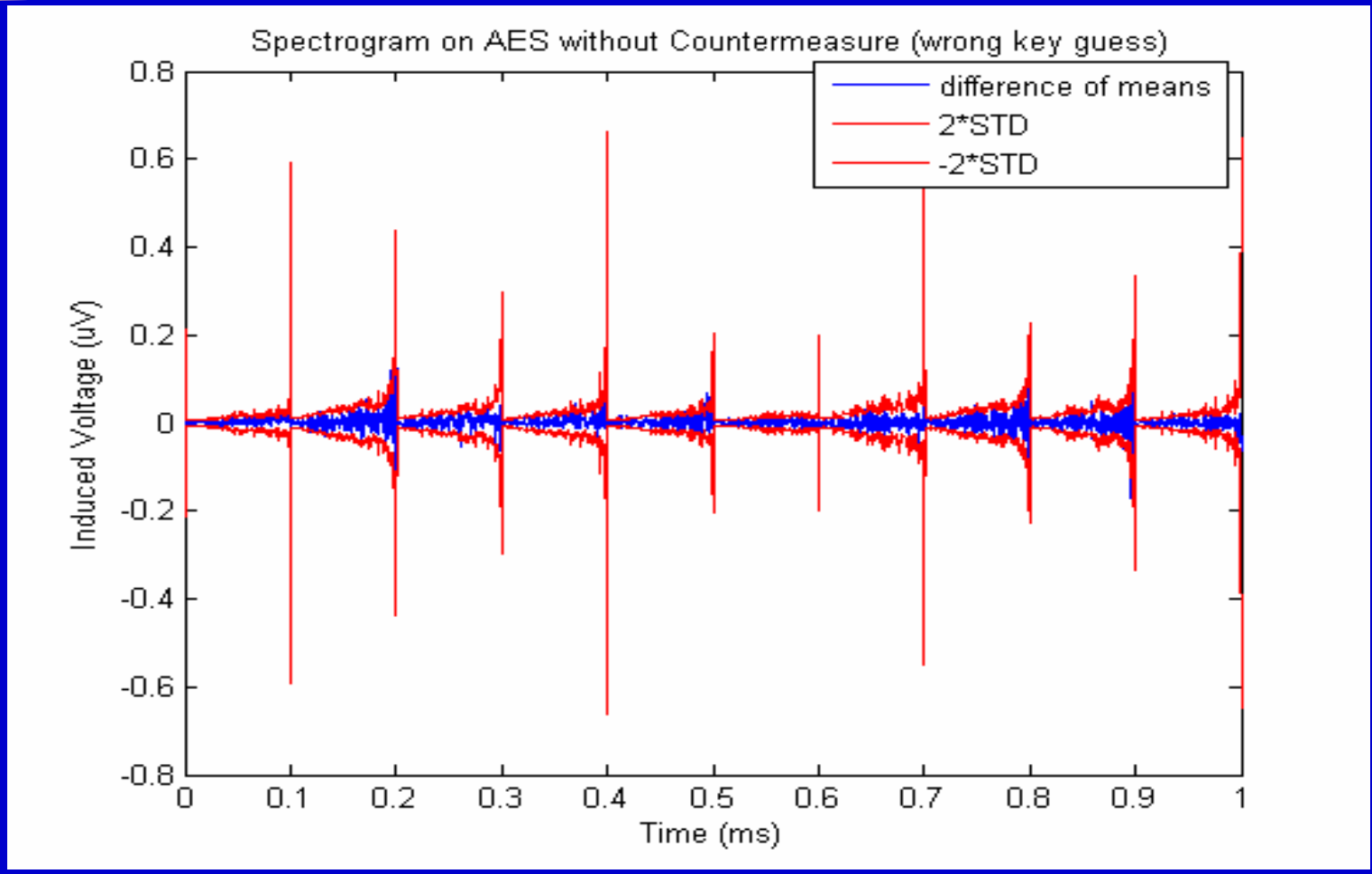
Differential Analysis of Rijndael



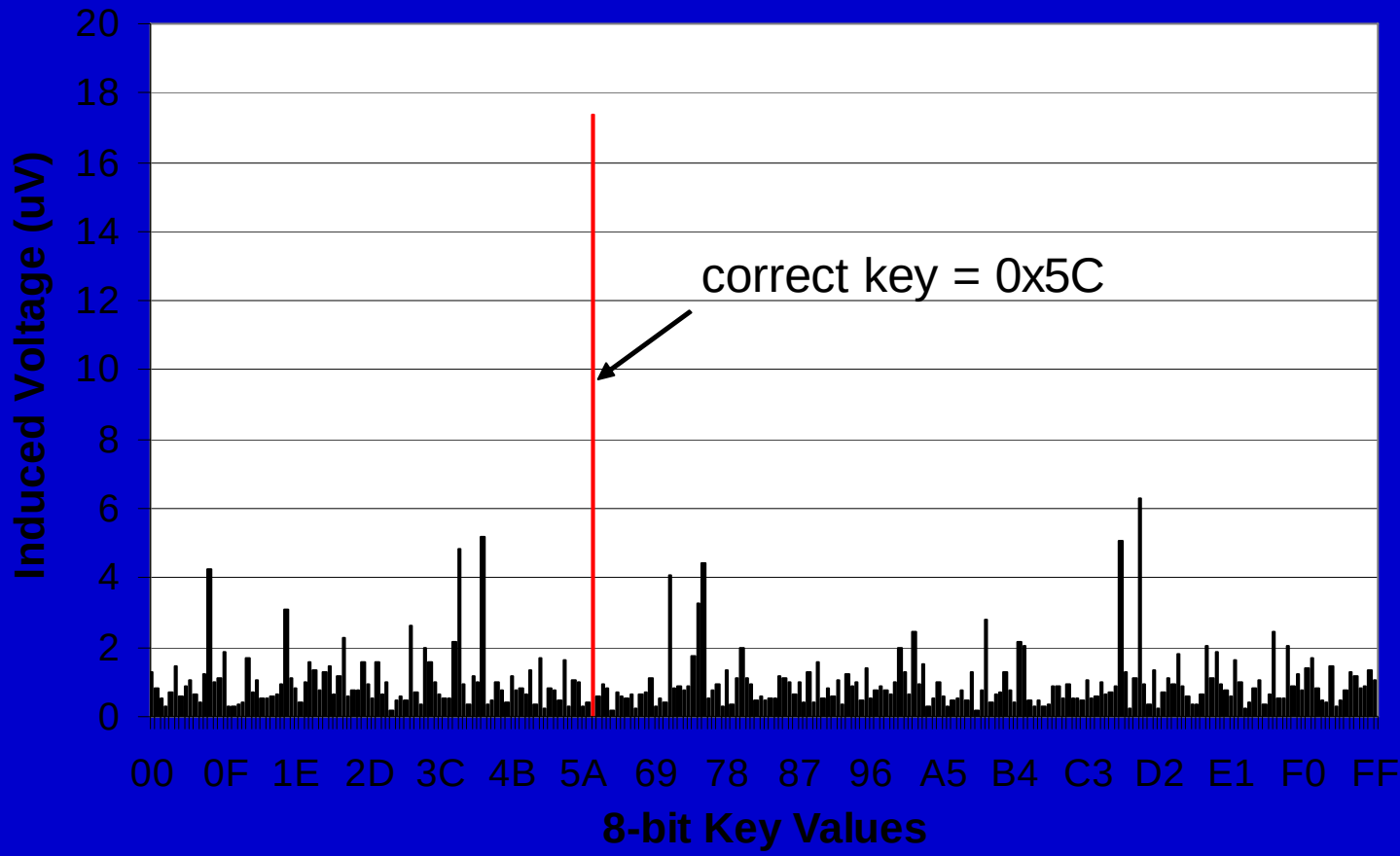
EM Frequency-based Differential for Correct Key



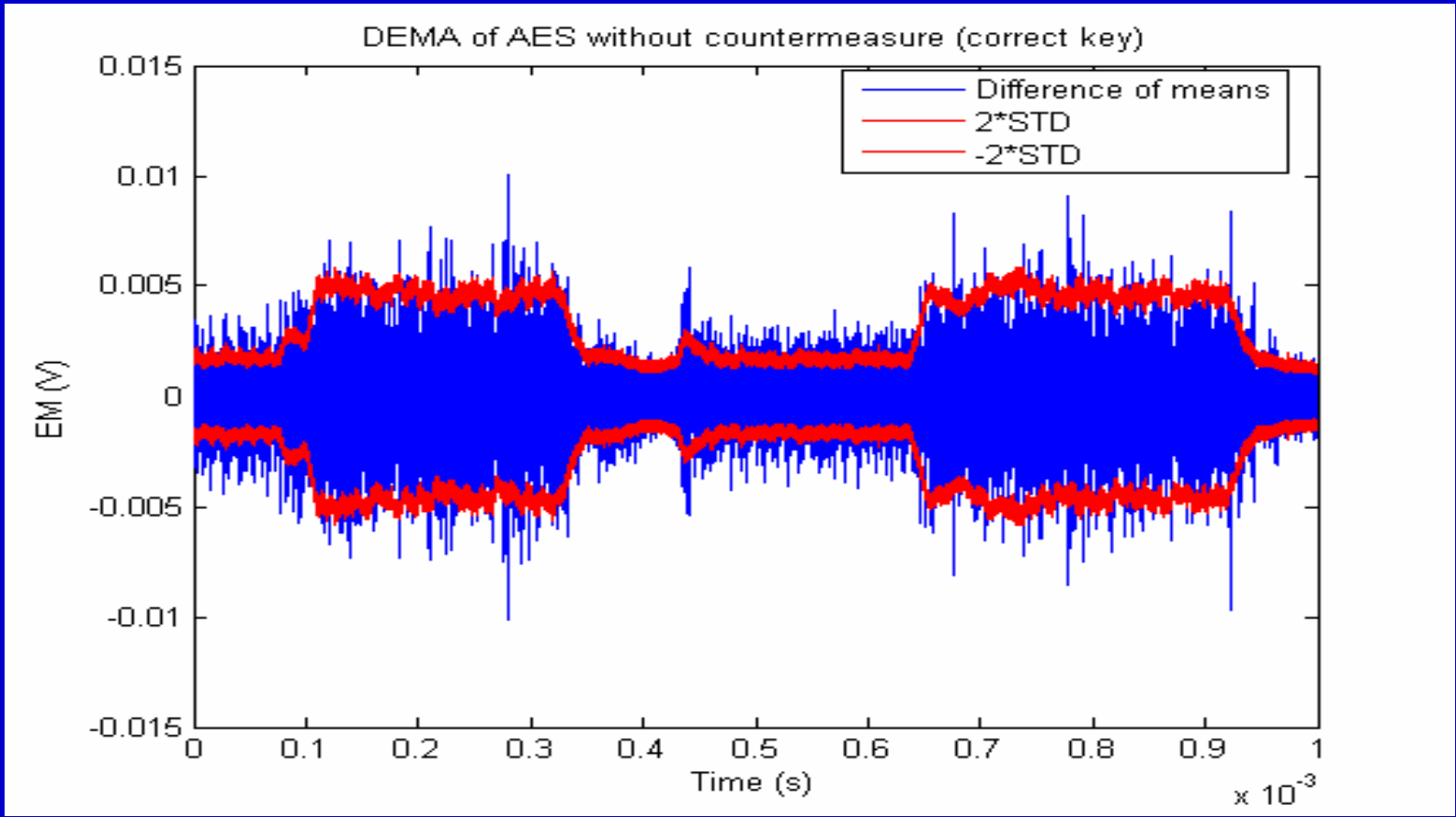
EM Frequency-based Differential for Incorrect Key



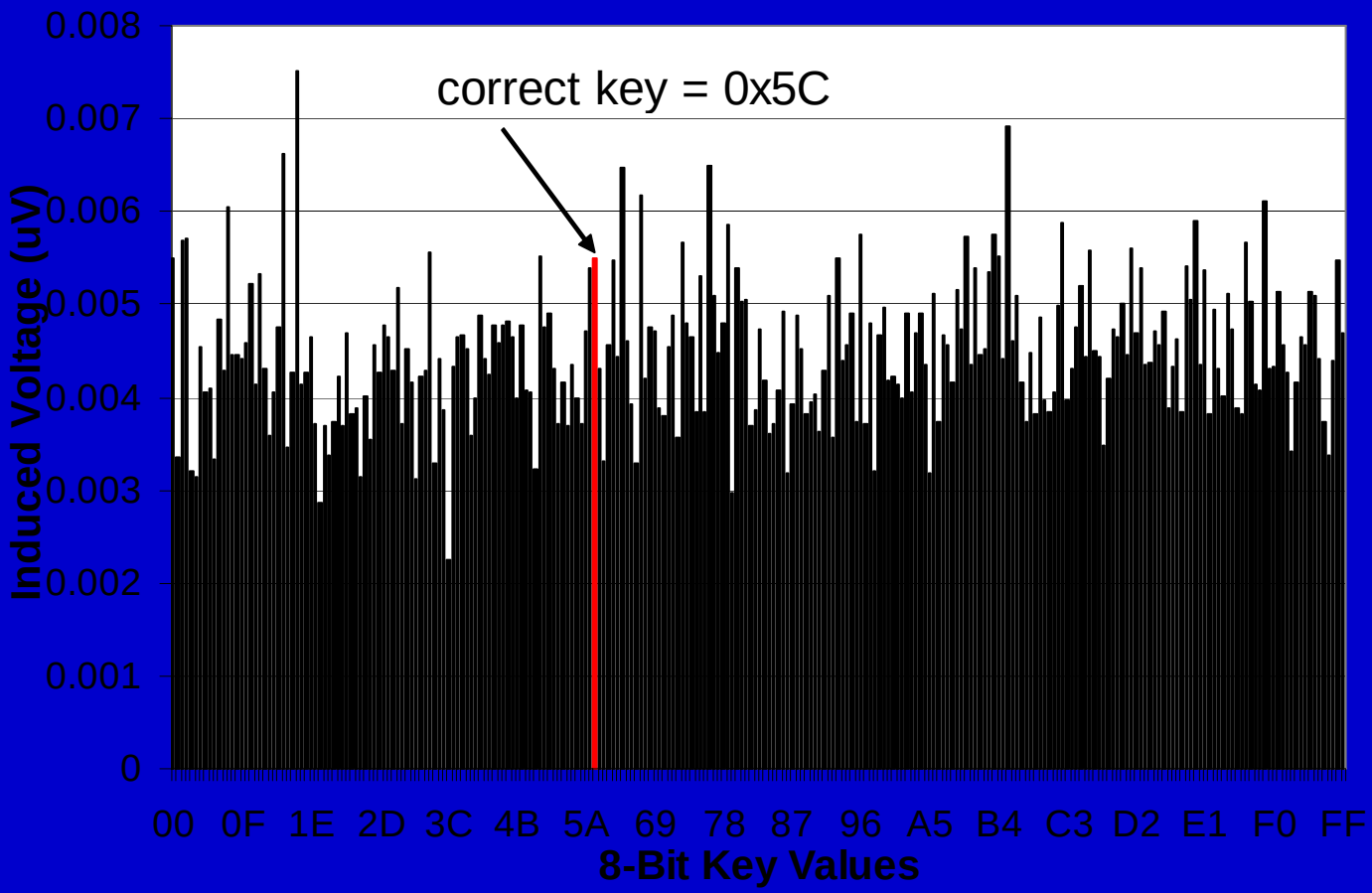
All Keys Guess for EM Frequency-based Differential Analysis



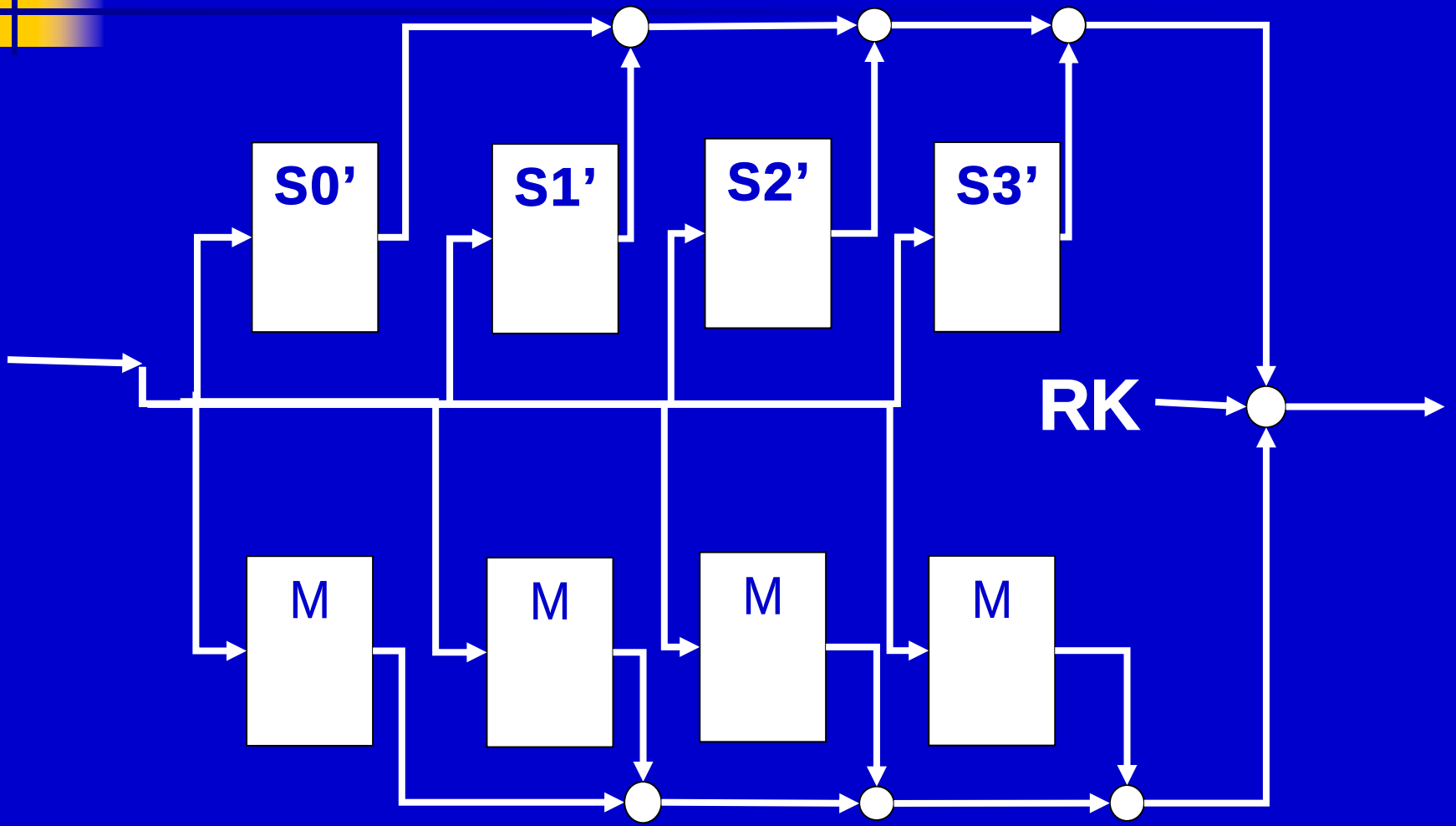
EM Time-based Differential for Correct Key



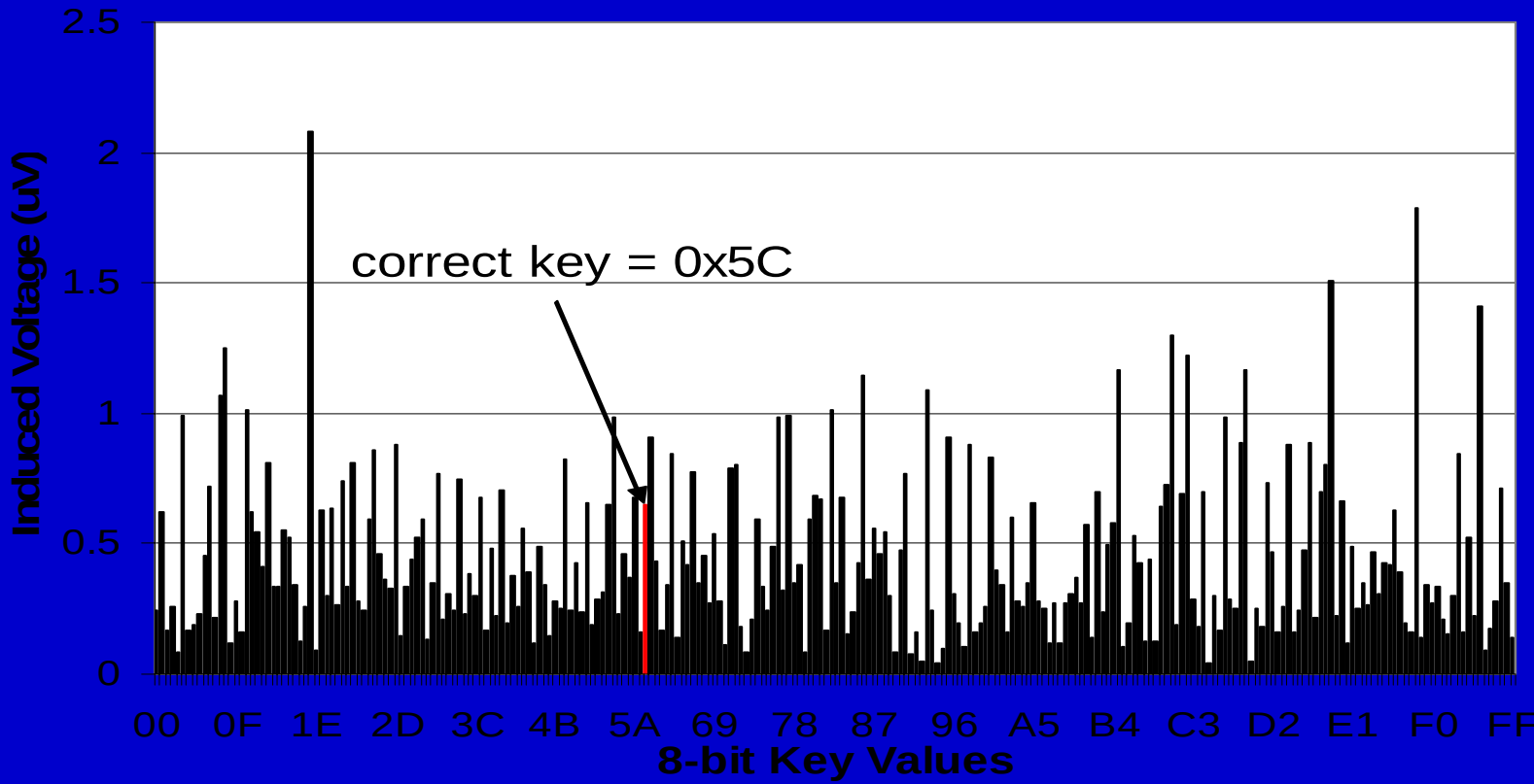
All Keys Guess for EM Time-based Differential Analysis



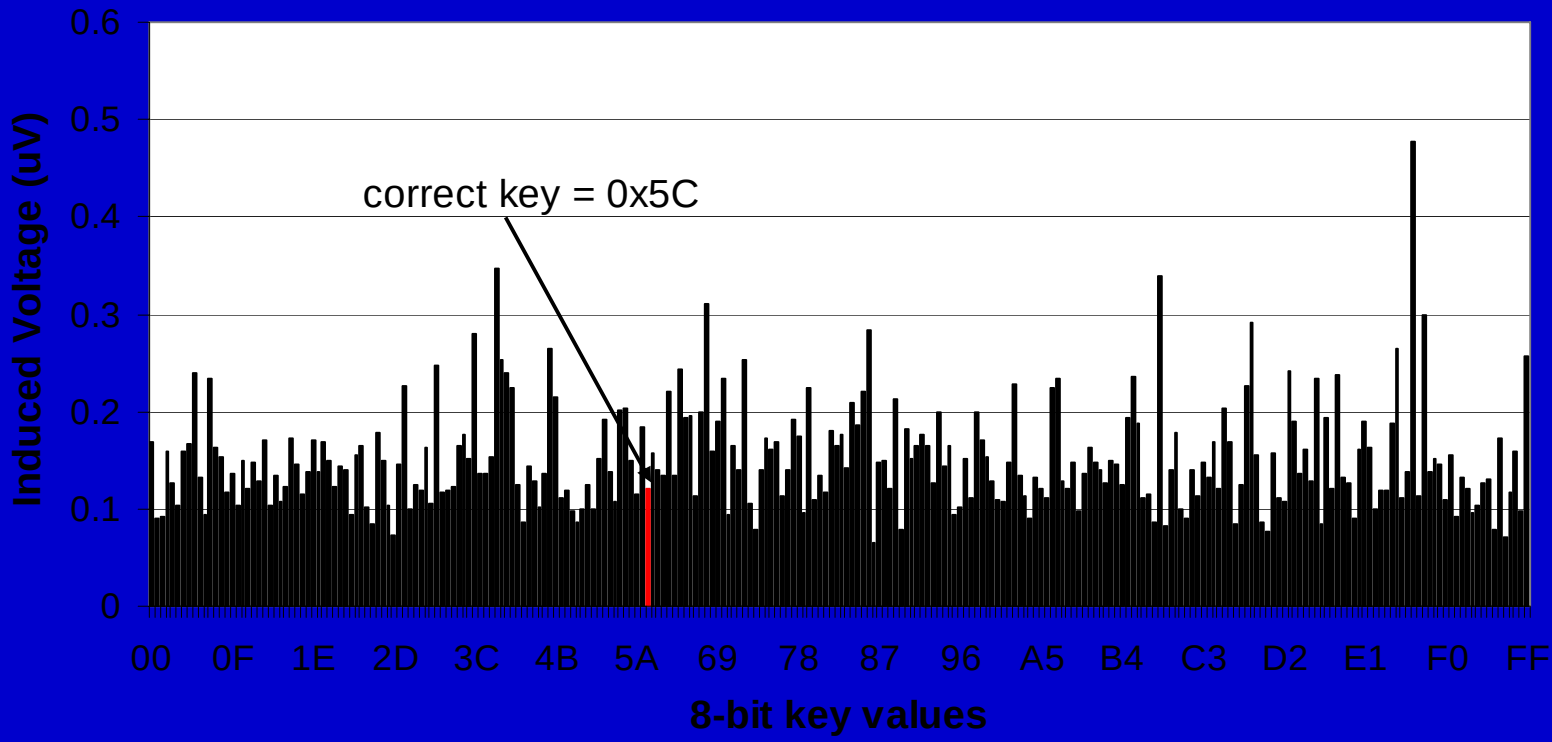
Countermeasure in Rijndael



All Keys Guess for EM Frequency-based Differential Analysis with Countermeasure



2nd Order EM Analysis with Countermeasure (Waddle 2004)

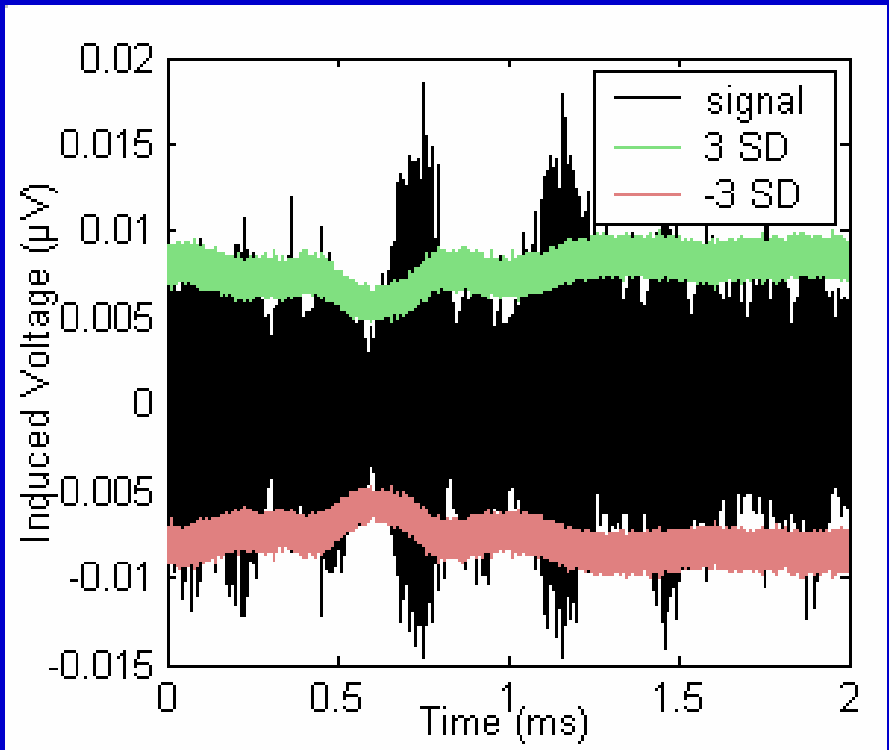


Countermeasure Energy

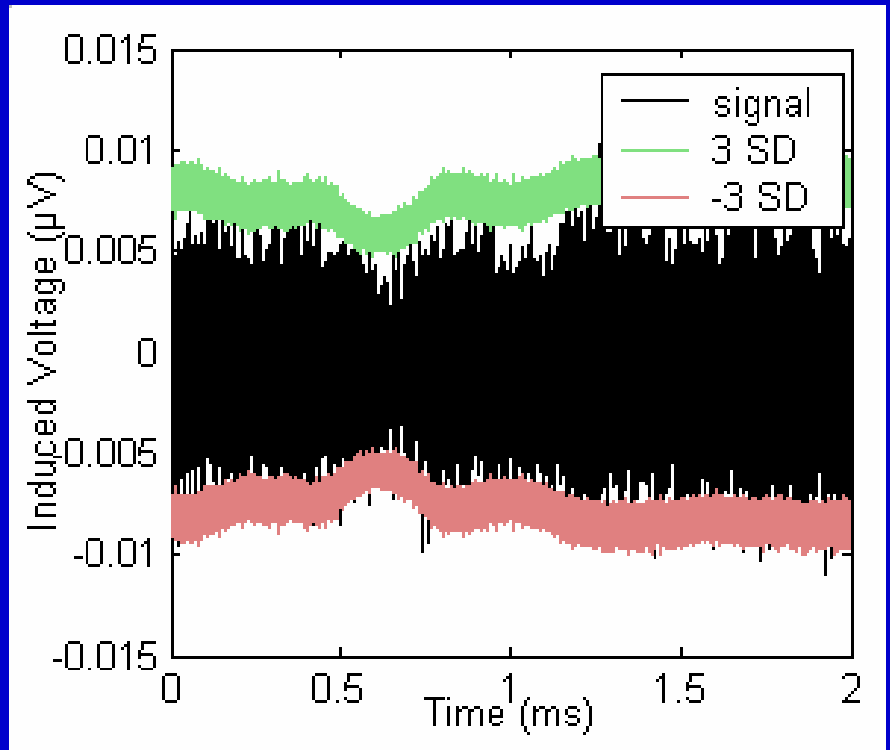
	Rijndael	C1	C2	(Messerges 2001)
# Sbox	5	6	7	5
# ld/st	160	320	480	2048
I (mA)	4.46	4.41	4.40	4.17
E_p *(mJ)*	0.33	0.57	0.81	2.92
E times	1	1.7	2.4	8.9

EM Time-based Differential for ECC

Correct

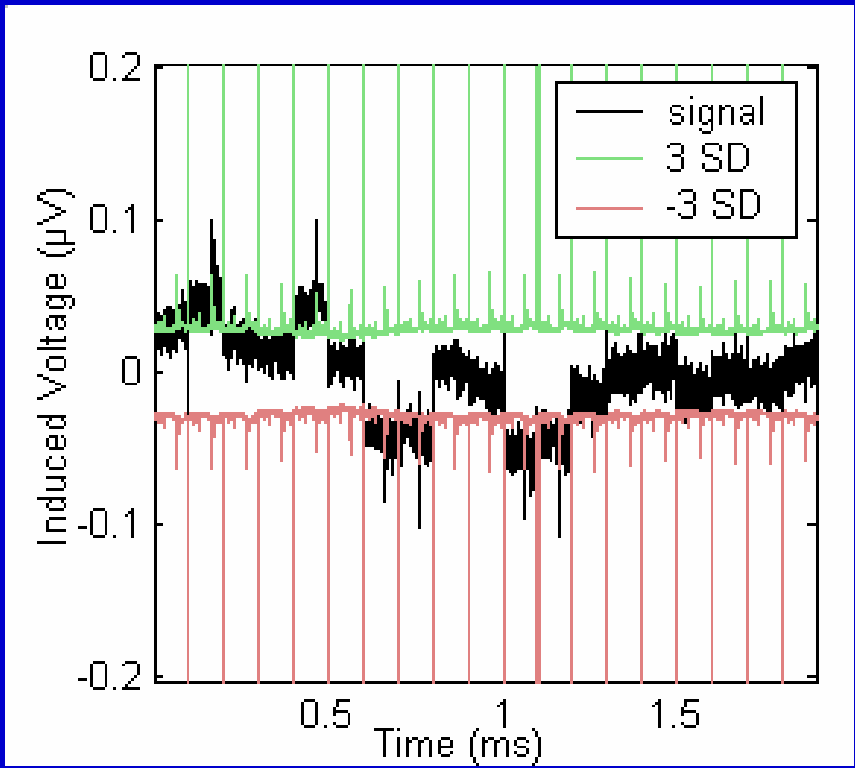


Incorrect

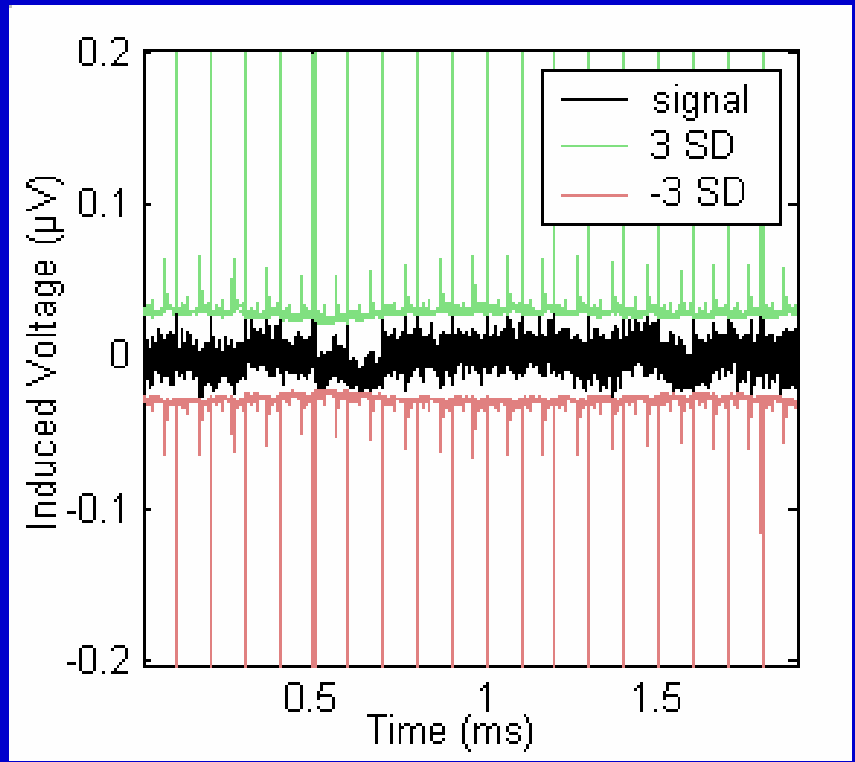


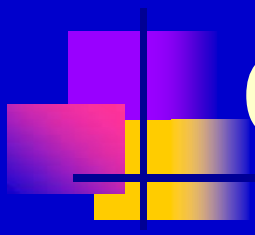
EM Frequency-based Differential for ECC

Correct



Incorrect





Conclusions

- Evaluated PDA side-channel
  - SEMA of AES on a PDA
- Proposed a spectrogram-based analysis
  - DSA of AES on PDA
  - MSB attack for ECC
- Proposed low energy countermeasure
- Low energy security for wireless embedded systems