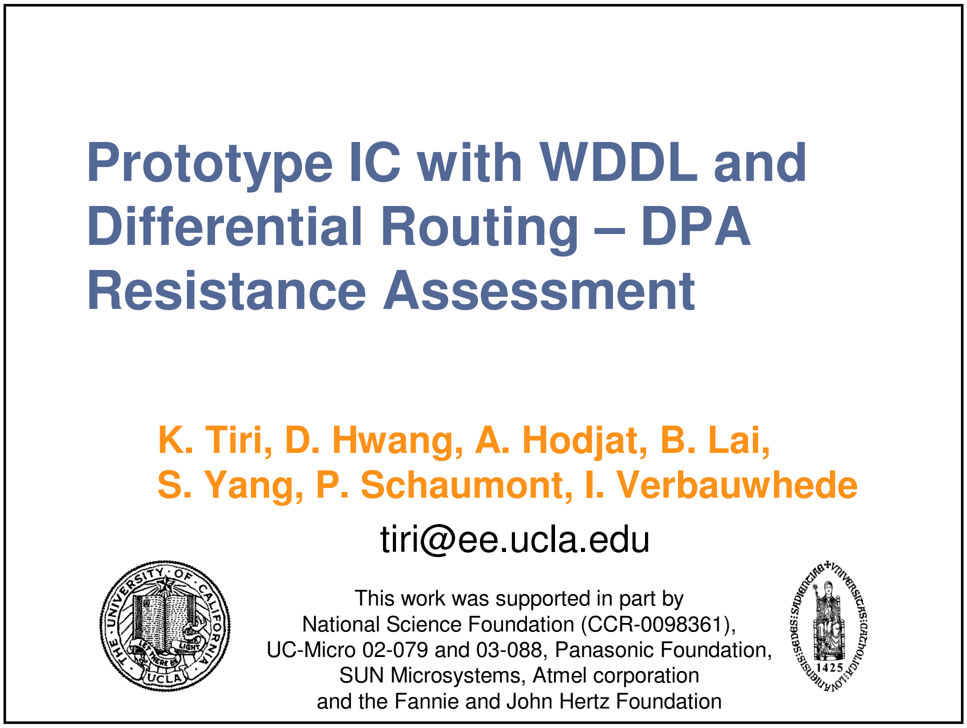
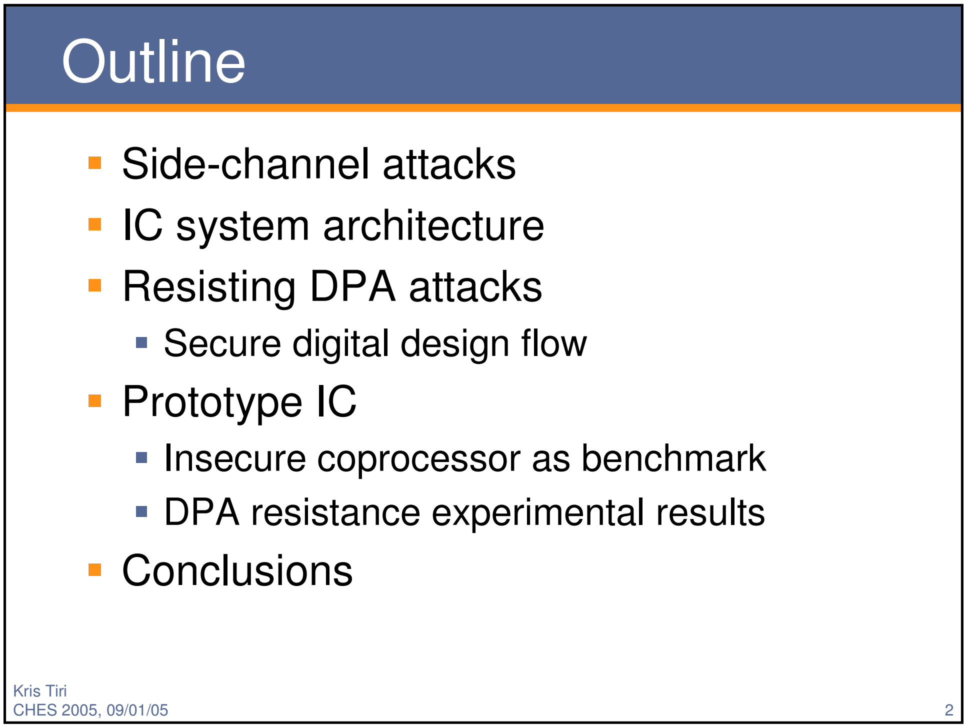


Prototype IC with WDDL and Differential Routing – DPA Resistance Assessment

K. Tiri, D. Hwang, A. Hodjat, B. Lai,
S. Yang, P. Schaumont, I. Verbauwhede

tiri@ee.ucla.edu

This work was supported in part by
National Science Foundation (CCR-0098361),
UC-Micro 02-079 and 03-088, Panasonic Foundation,
SUN Microsystems, Atmel corporation
and the Fannie and John Hertz Foundation

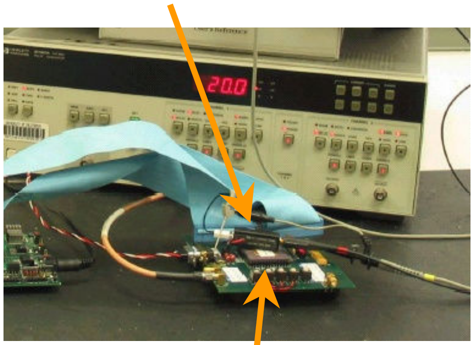


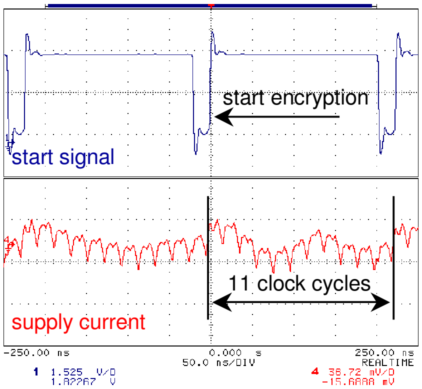
Outline

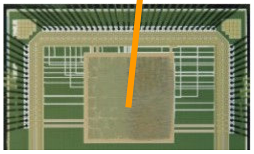
- Side-channel attacks
- IC system architecture
- Resisting DPA attacks
  - Secure digital design flow
- Prototype IC
  - Insecure coprocessor as benchmark
  - DPA resistance experimental results
- Conclusions

Side-channel attacks

Current Probe

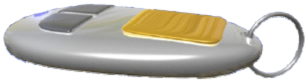


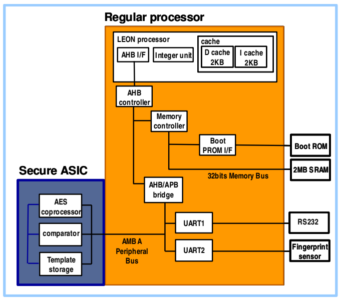




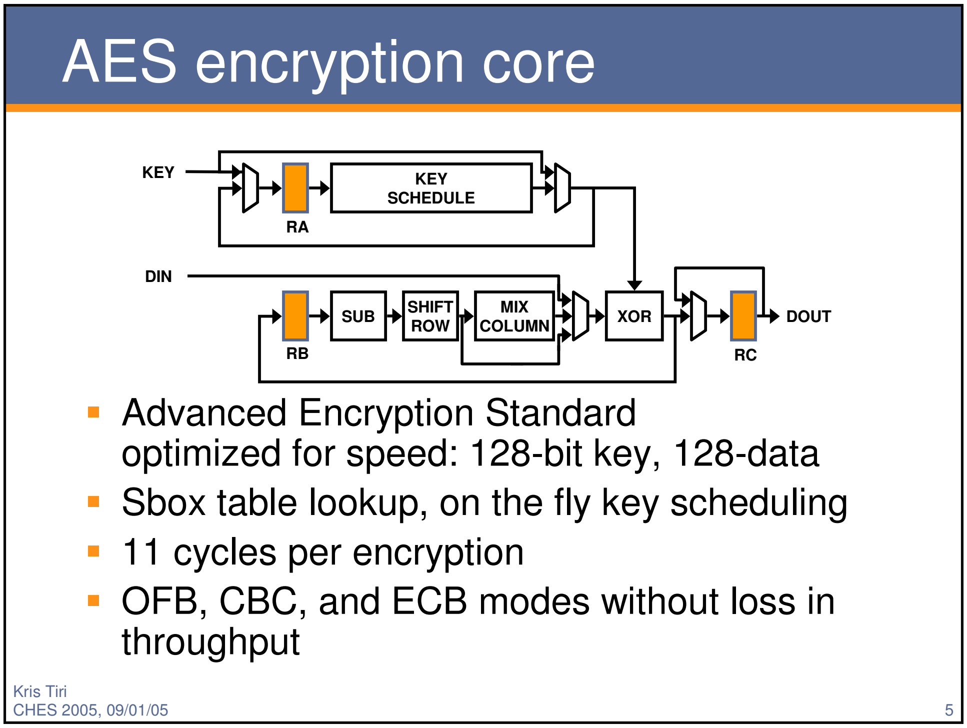
- 128-bit AES encryption cracked under 3 min.

ThumbPod device



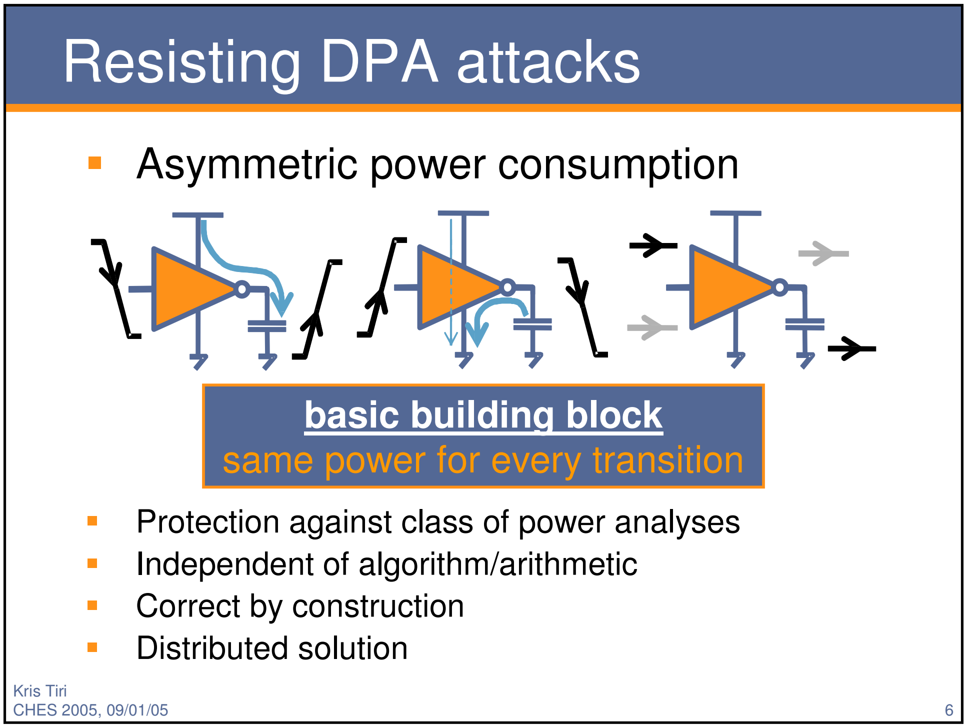


- Biometrically-driven electronic key
- Strong, secure bond between owner and key
- Components:
  - Microprocessor
  - Fingerprint sensor
  - Wireless transceiver
  - Secure coprocessor
- Security partitioning



AES encryption core

- Advanced Encryption Standard optimized for speed: 128-bit key, 128-data
- Sbox table lookup, on the fly key scheduling
- 11 cycles per encryption
- OFB, CBC, and ECB modes without loss in throughput

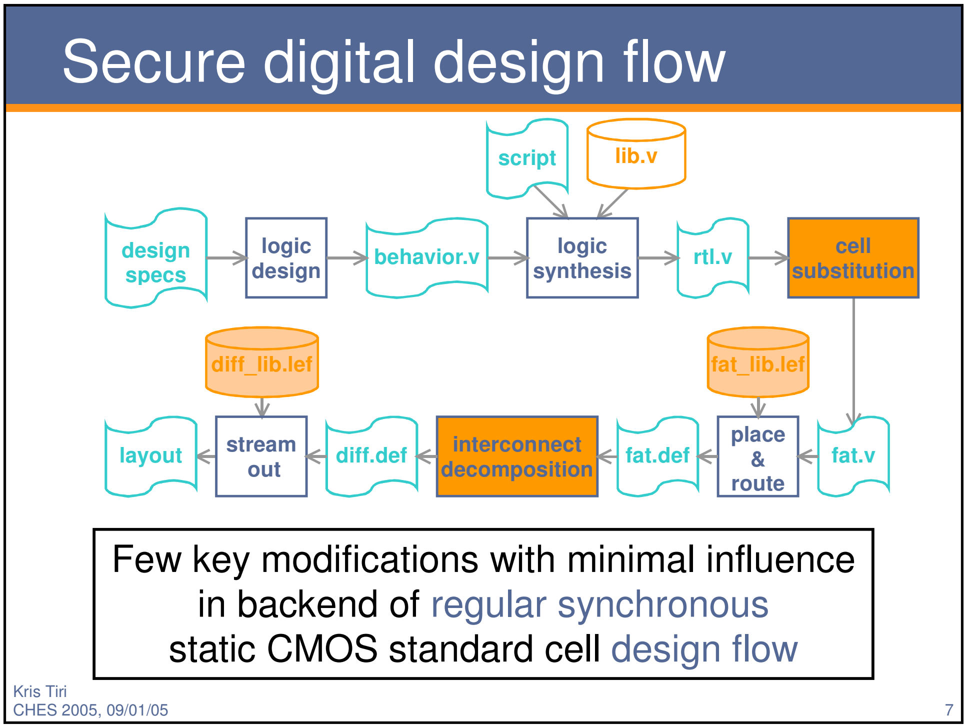


Resisting DPA attacks

- Asymmetric power consumption

basic building block
same power for every transition

- Protection against class of power analyses
- Independent of algorithm/arithmetic
- Correct by construction
- Distributed solution



Secure digital design flow

design specs → logic design → behavior.v → logic synthesis → rtl.v → cell substitution

script, lib.v → logic synthesis

cell substitution → fat.v → place & route → fat.def → interconnect decomposition → diff.def → stream out → layout

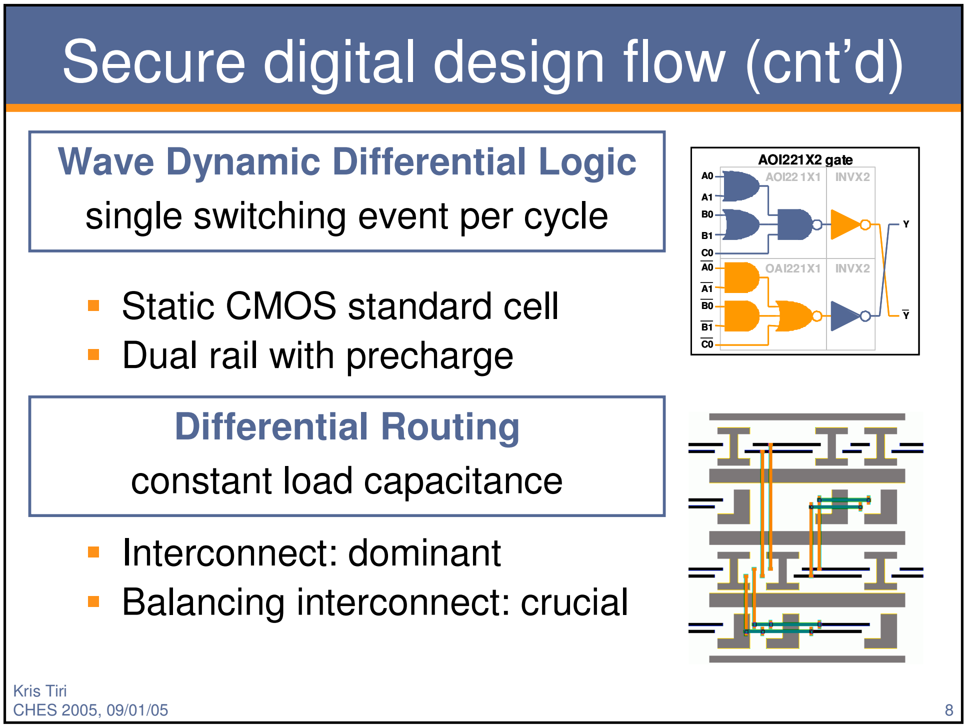
fat_lib.lef → place & route

diff_lib.lef → stream out

Few key modifications with minimal influence in backend of regular synchronous static CMOS standard cell design flow

Kris Tiri
CHES 2005, 09/01/05

7



Secure digital design flow (cnt'd)

Wave Dynamic Differential Logic

single switching event per cycle

- Static CMOS standard cell
- Dual rail with precharge

Differential Routing

constant load capacitance

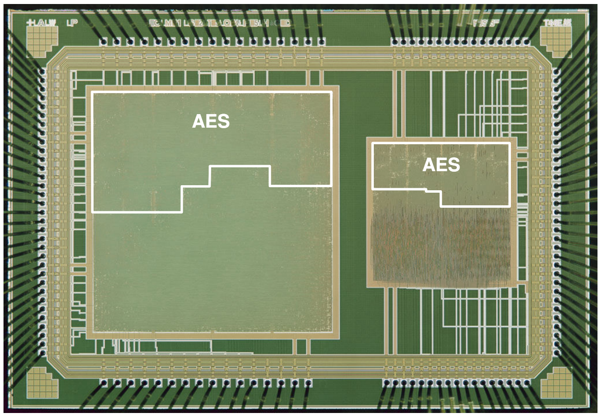
- Interconnect: dominant
- Balancing interconnect: crucial

Kris Tiri
CHES 2005, 09/01/05

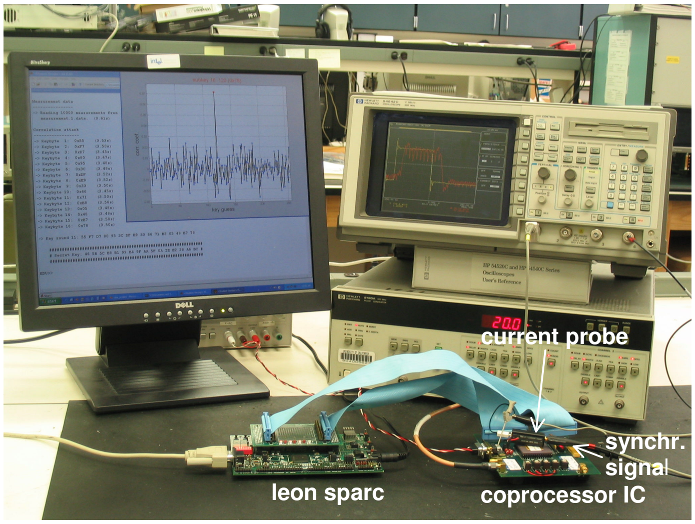
8

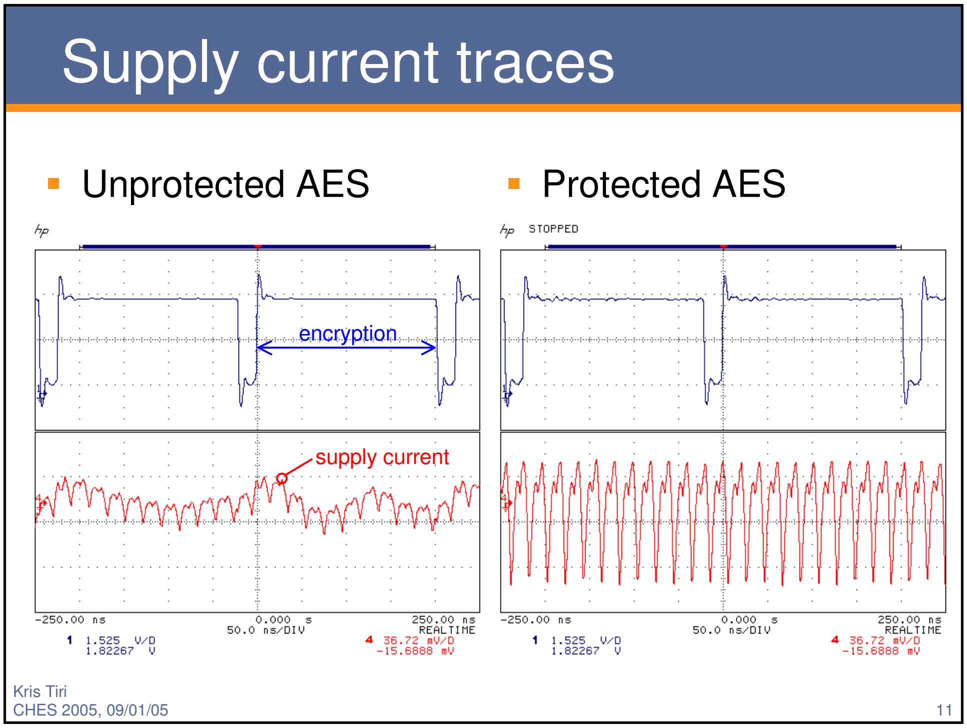
Prototype IC in 0.18µm CMOS

- WDDL, differential route
- Single-ended, regular route



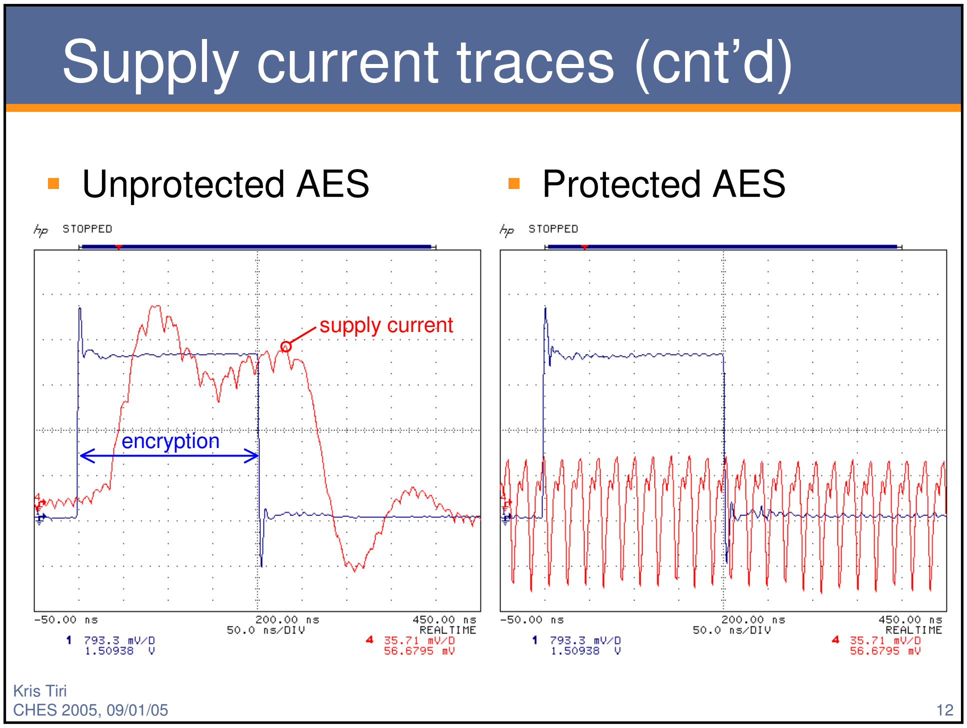
DPA attack setup





Supply current traces

- Unprotected AES
- Protected AES



Supply current traces (cnt'd)

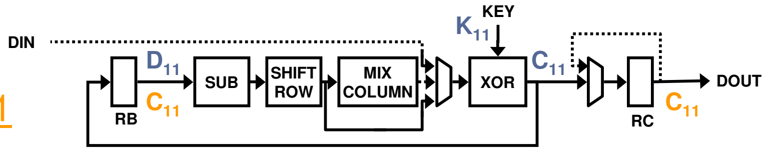
- Unprotected AES
- Protected AES

DPA resistance assessment

- Estimate power consumption in round 11 + 1

R11

R11+1



- Compare Hamming distances & measurements

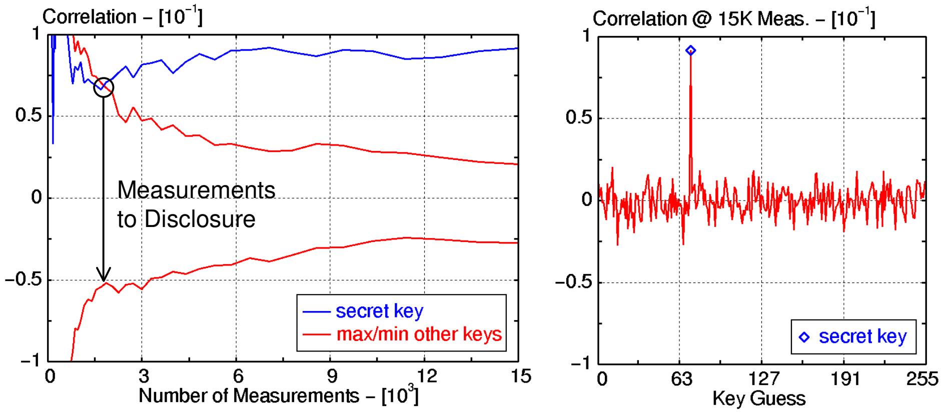
$$\max_{K_{11}} f_{cost}(K_{11}) = \mathrm{corr}(P_{measurement},P_{estimation})$$

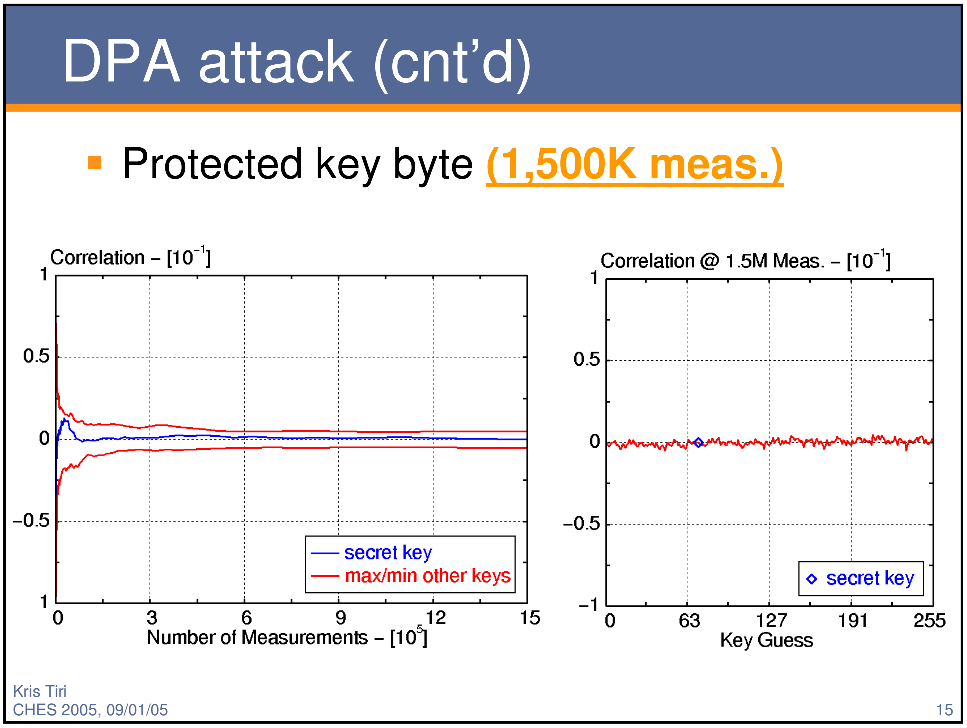
$$\begin{aligned} \textit{where}\quad & P_{measurement} = \max(I_{supply,11+1}) \\ & P_{estimation} = \mathrm{HamDist}(D_{11},C_{11}) \\ & D_{11} = \mathrm{sub}^{-1}(\mathrm{shiftrow}^{-1}(K_{11} \otimes C_{11})) \end{aligned}$$

- $16*2^8$ key guesses vs. 2^{128} key guesses

DPA attack

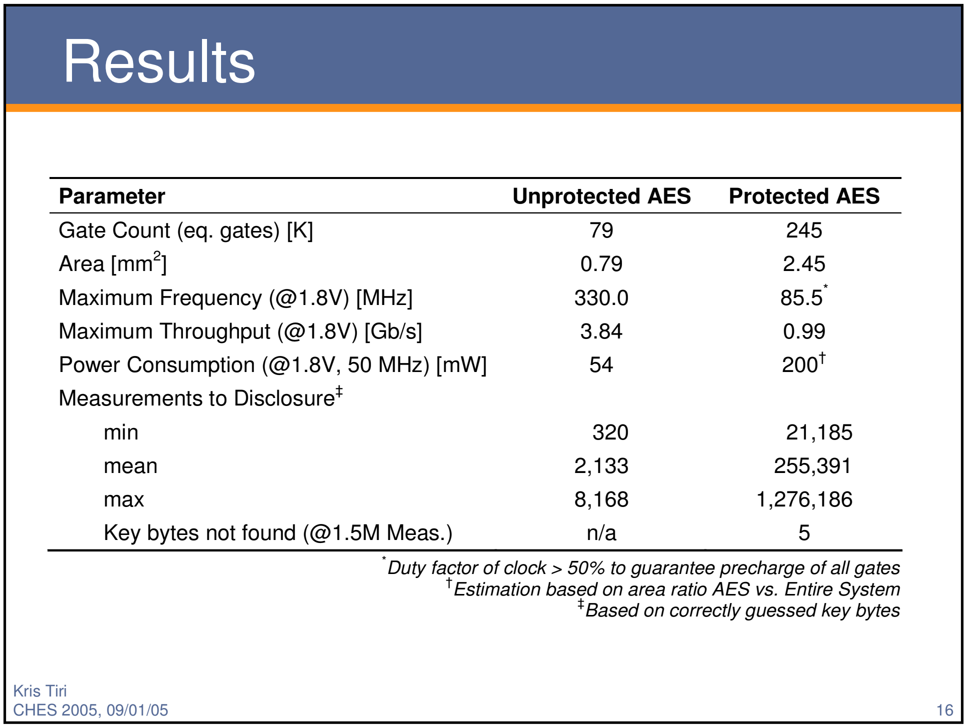
- Unprotected key byte (15K meas.)





DPA attack (cnt'd)

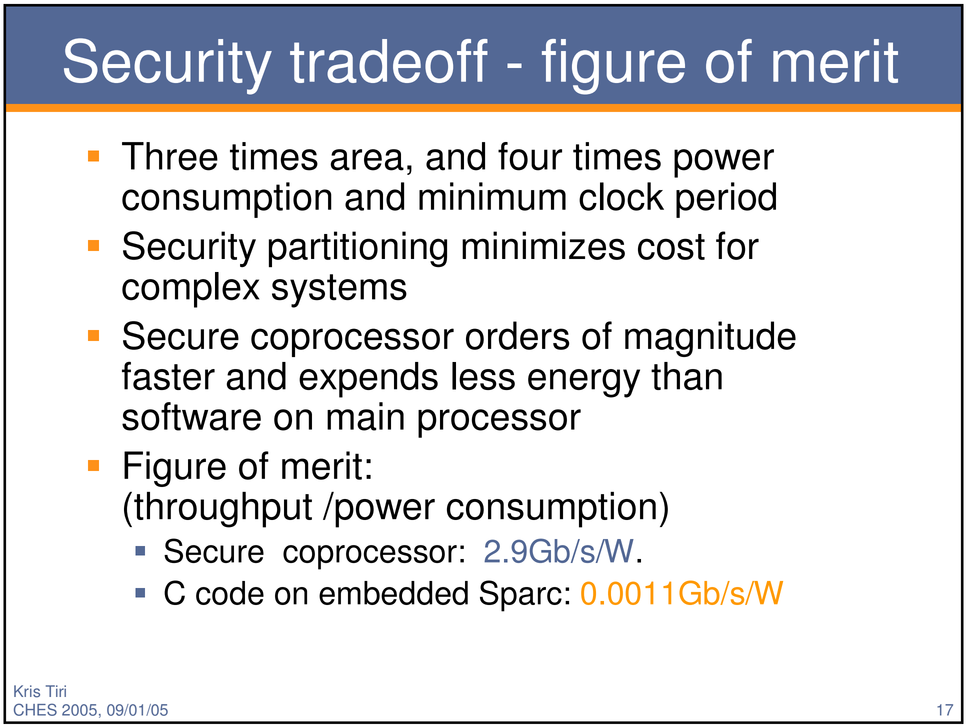
- Protected key byte **(1,500K meas.)**



Results

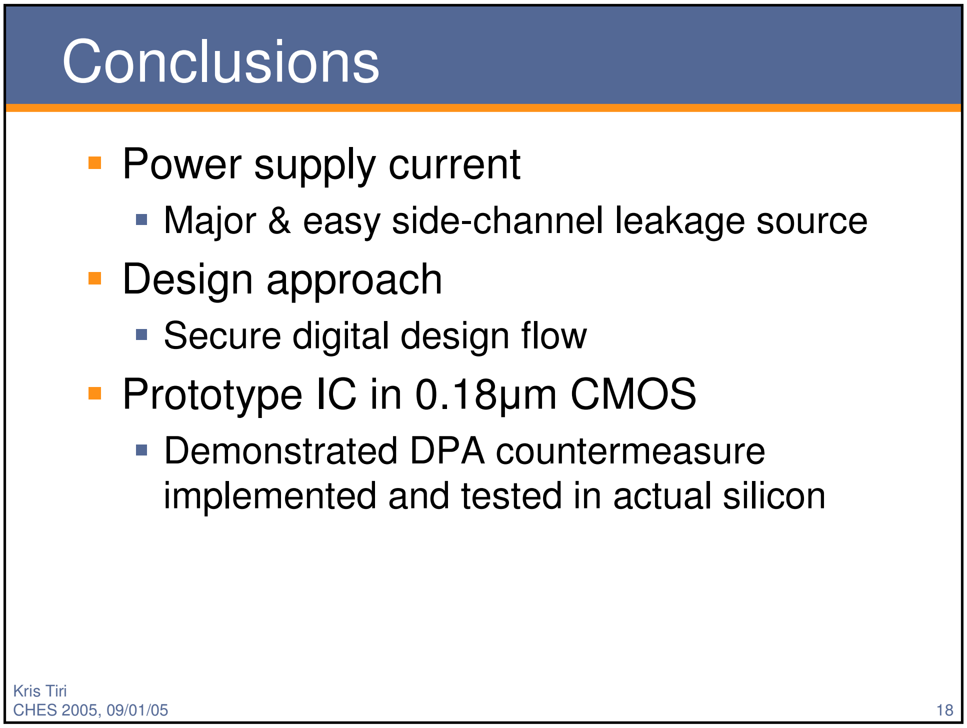
Parameter	Unprotected AES	Protected AES
Gate Count (eq. gates) [K]	79	245
Area [mm^2]	0.79	2.45
Maximum Frequency (@1.8V) [MHz]	330.0	85.5[*]
Maximum Throughput (@1.8V) [Gb/s]	3.84	0.99
Power Consumption (@1.8V, 50 MHz) [mW]	54	200[†]
Measurements to Disclosure[‡]		
min	320	21,185
mean	2,133	255,391
max	8,168	1,276,186
Key bytes not found (@1.5M Meas.)	n/a	5

[*] *Duty factor of clock > 50% to guarantee precharge of all gates*
[†] *Estimation based on area ratio AES vs. Entire System*
[‡] *Based on correctly guessed key bytes*



Security tradeoff - figure of merit

- Three times area, and four times power consumption and minimum clock period
- Security partitioning minimizes cost for complex systems
- Secure coprocessor orders of magnitude faster and expends less energy than software on main processor
- Figure of merit:
  (throughput /power consumption)
  - Secure coprocessor: 2.9Gb/s/W.
  - C code on embedded Sparc: 0.0011Gb/s/W



Conclusions

- Power supply current
  - Major & easy side-channel leakage source
- Design approach
  - Secure digital design flow
- Prototype IC in 0.18µm CMOS
  - Demonstrated DPA countermeasure implemented and tested in actual silicon