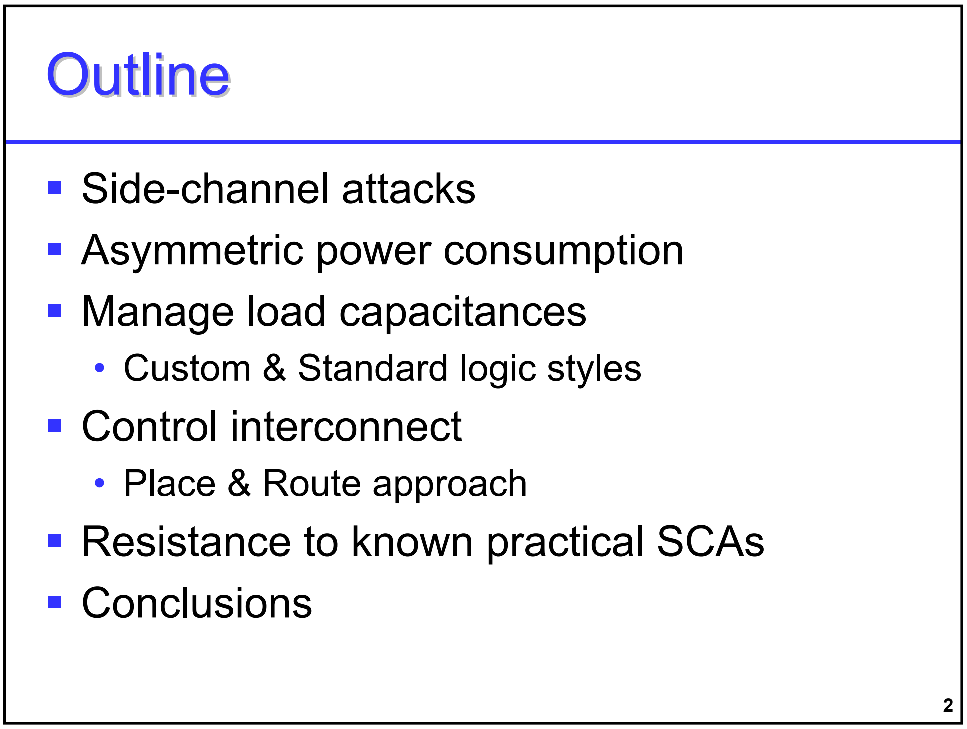
Hardware Countermeasures against Side-Channel Attacks

Kris Tiri

UC Los Angeles

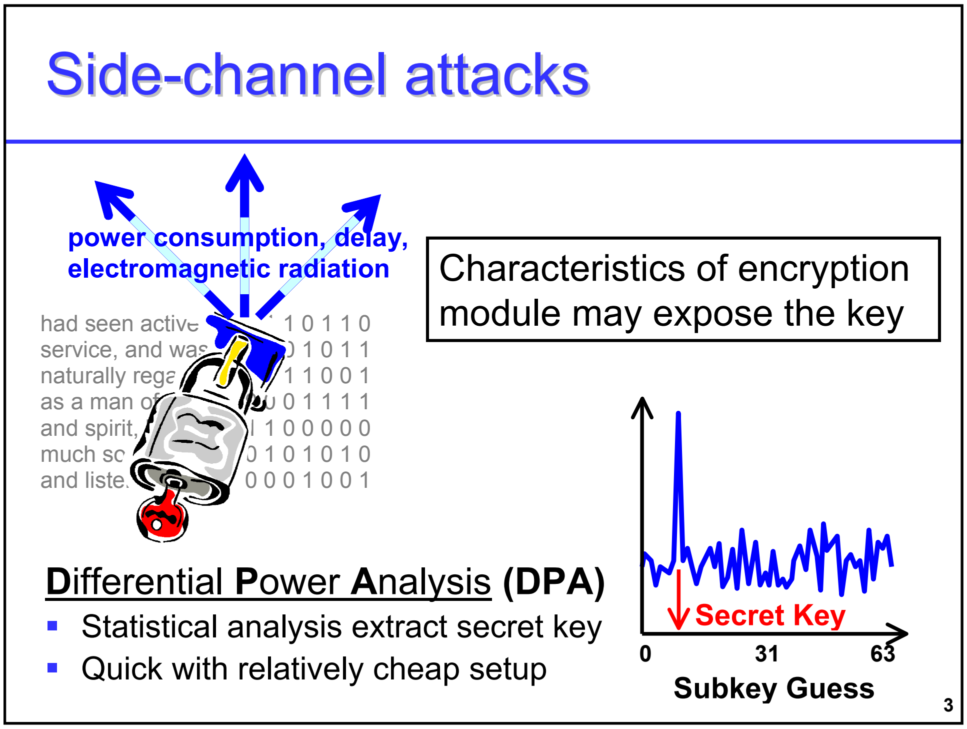
tiri@ee.ucla.edu



Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions

2

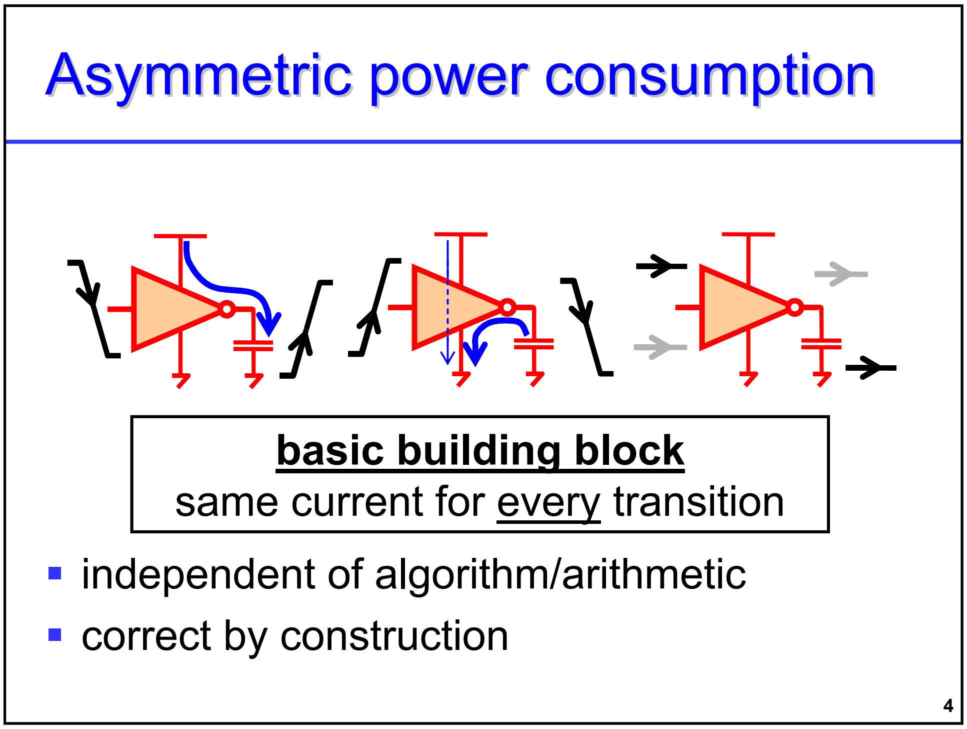


Side-channel attacks

Characteristics of encryption module may expose the key

Differential Power Analysis (DPA)

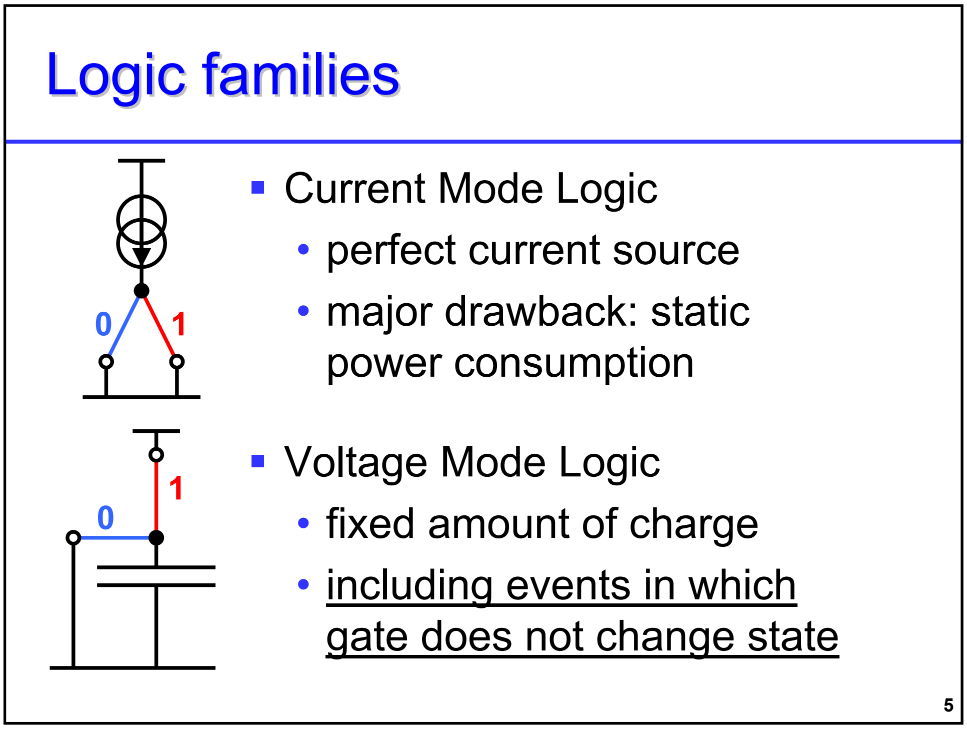
- Statistical analysis extract secret key
- Quick with relatively cheap setup



Asymmetric power consumption

basic building block
same current for every transition

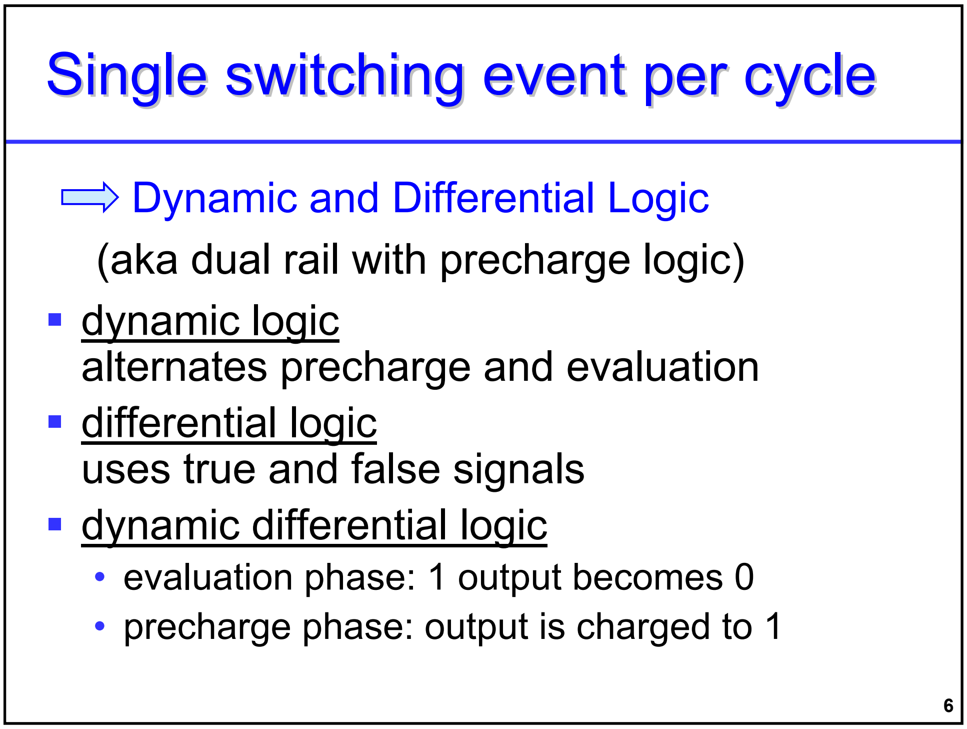
- independent of algorithm/arithmetic
- correct by construction



Logic families

- Current Mode Logic
  - perfect current source
  - major drawback: static power consumption
- Voltage Mode Logic
  - fixed amount of charge
  - including events in which gate does not change state

5



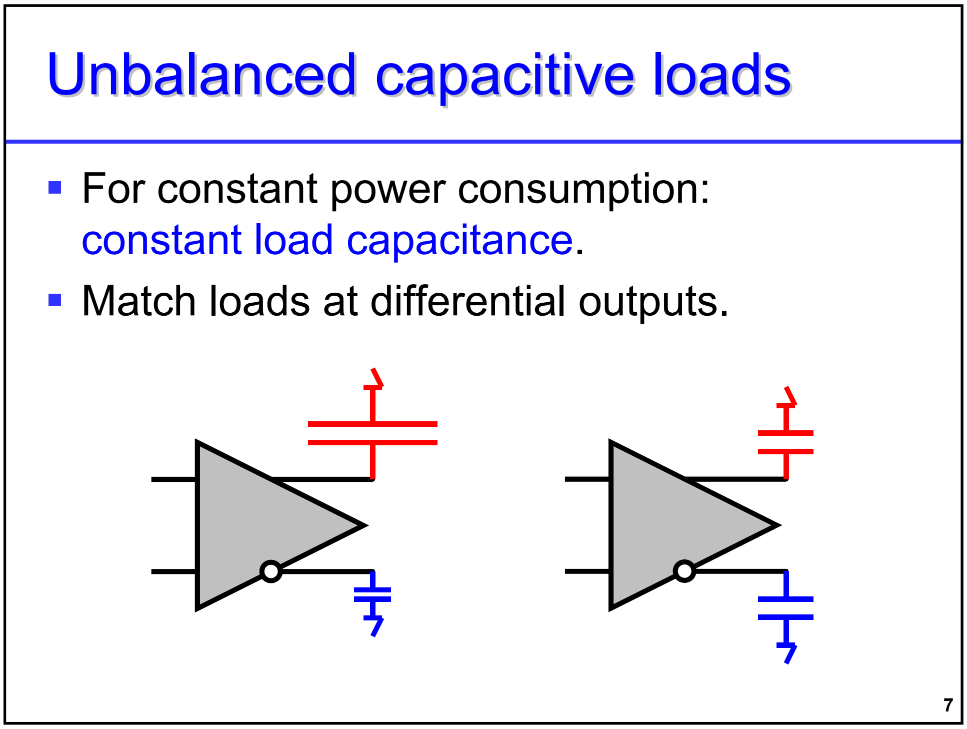
Single switching event per cycle

⇨ Dynamic and Differential Logic

(aka dual rail with precharge logic)

- dynamic logic
  alternates precharge and evaluation
- differential logic
  uses true and false signals
- dynamic differential logic
  - evaluation phase: 1 output becomes 0
  - precharge phase: output is charged to 1

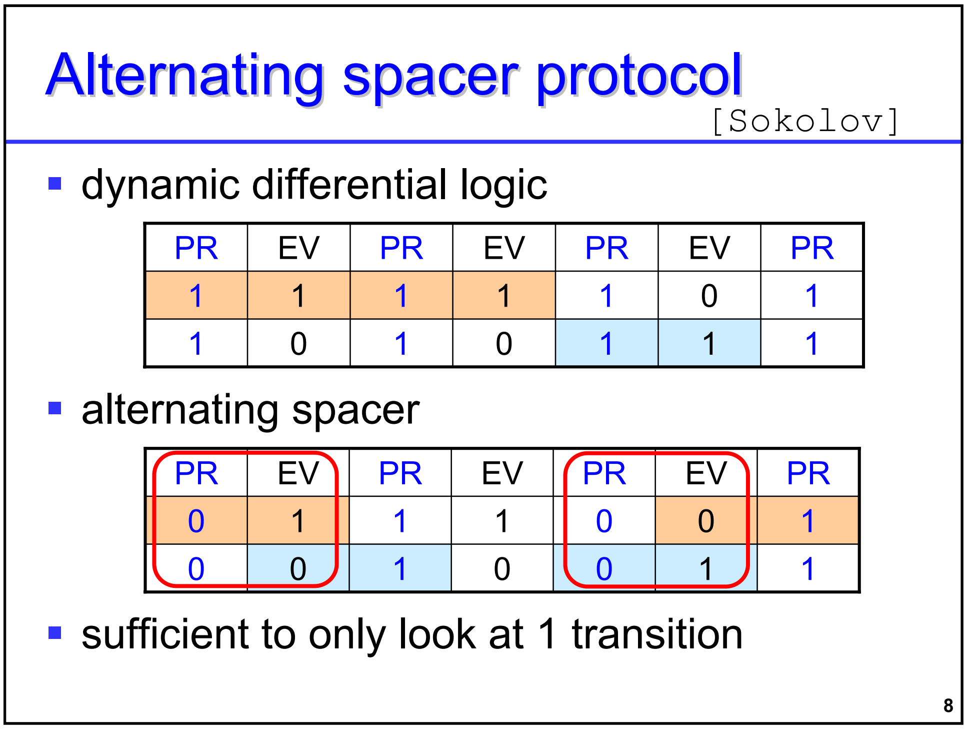
6



Unbalanced capacitive loads

- For constant power consumption: constant load capacitance.
- Match loads at differential outputs.

7



Alternating spacer protocol

[Sokolov]

- dynamic differential logic

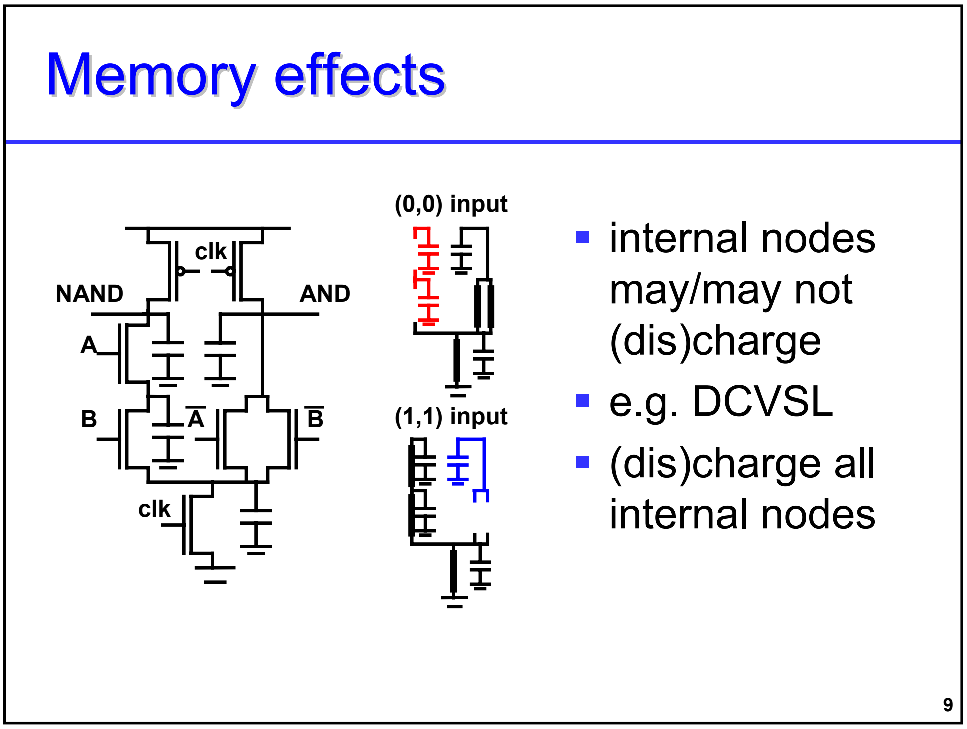
PR	EV	PR	EV	PR	EV	PR
1	1	1	1	1	0	1
1	0	1	0	1	1	1

- alternating spacer

PR	EV	PR	EV	PR	EV	PR
0	1	1	1	0	0	1
0	0	1	0	0	1	1

- sufficient to only look at 1 transition

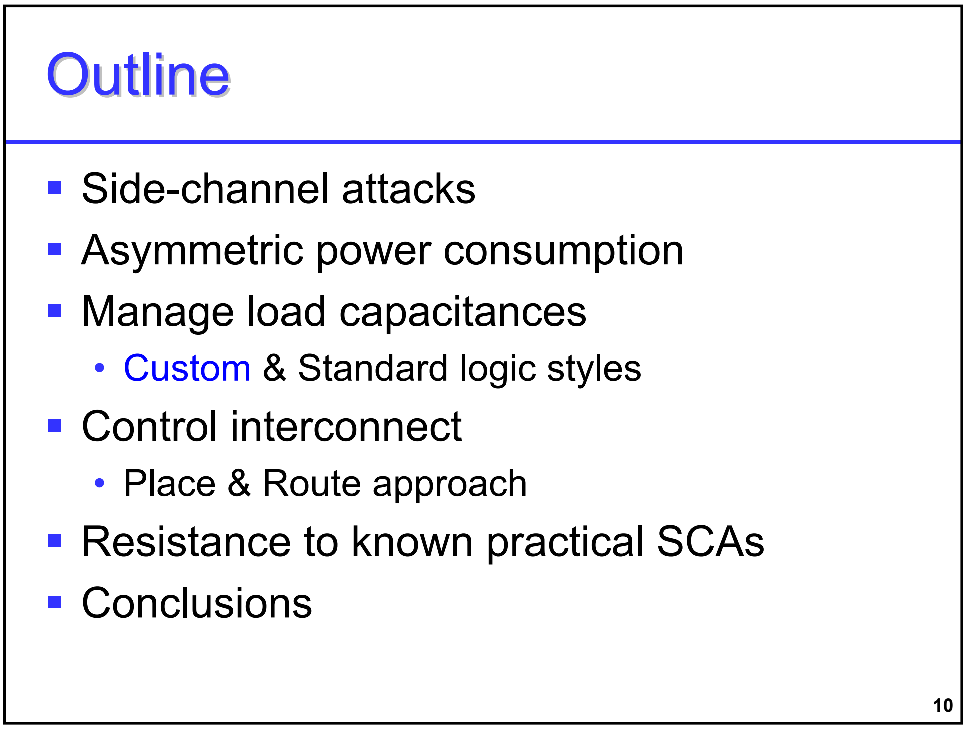
8



Memory effects

- internal nodes may/may not (dis)charge
- e.g. DCVSL
- (dis)charge all internal nodes

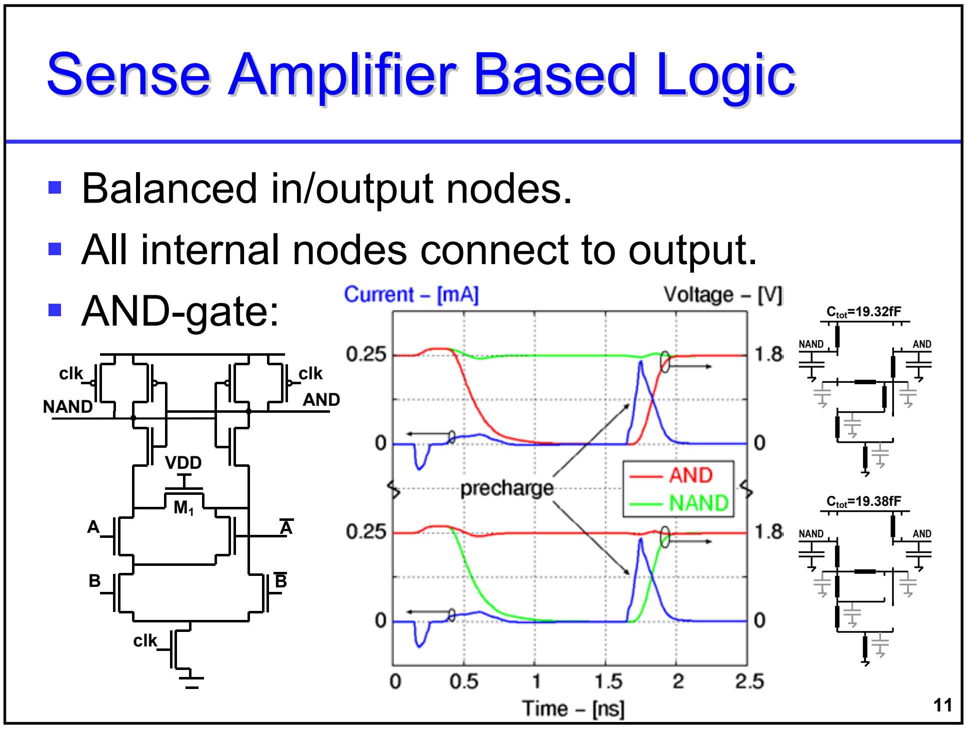
9



Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions

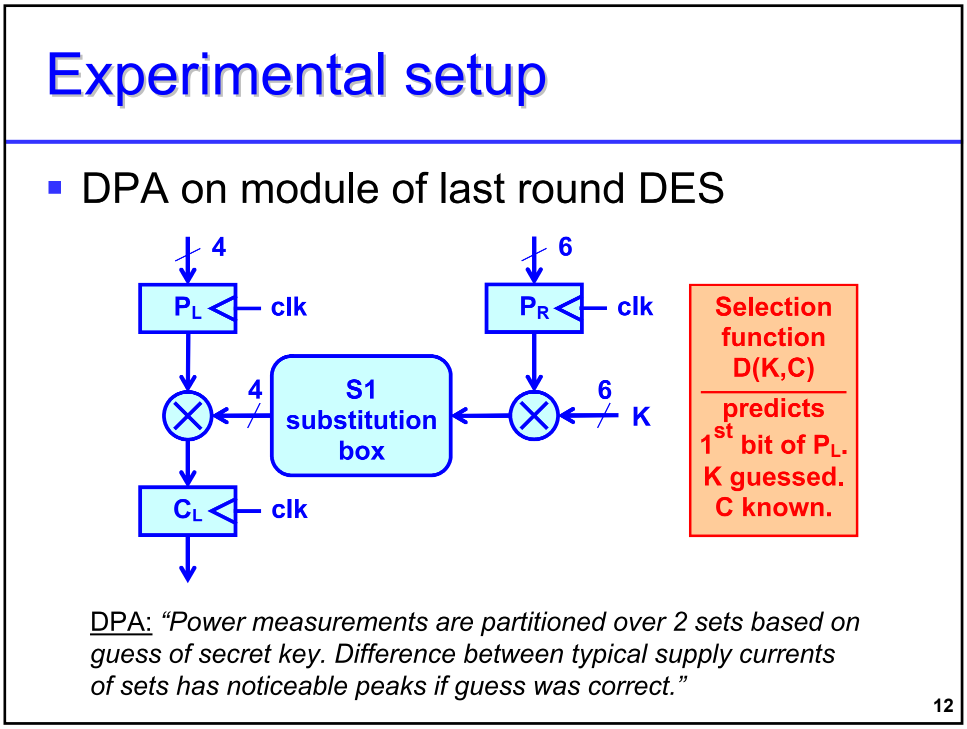
10



Sense Amplifier Based Logic

- Balanced in/output nodes.
- All internal nodes connect to output.
- AND-gate:

11



Experimental setup

- DPA on module of last round DES

Selection function D(K,C)

predicts 1st bit of P$_L$. K guessed. C known.

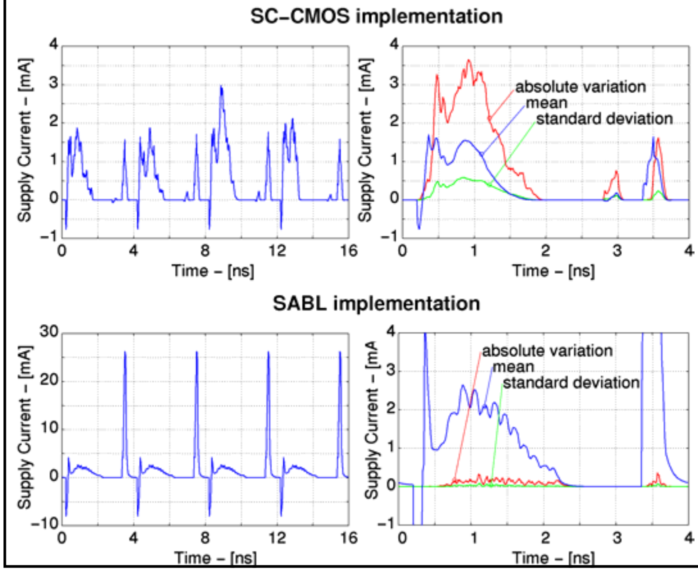
DPA: *“Power measurements are partitioned over 2 sets based on guess of secret key. Difference between typical supply currents of sets has noticeable peaks if guess was correct.”*

12

Implementation details

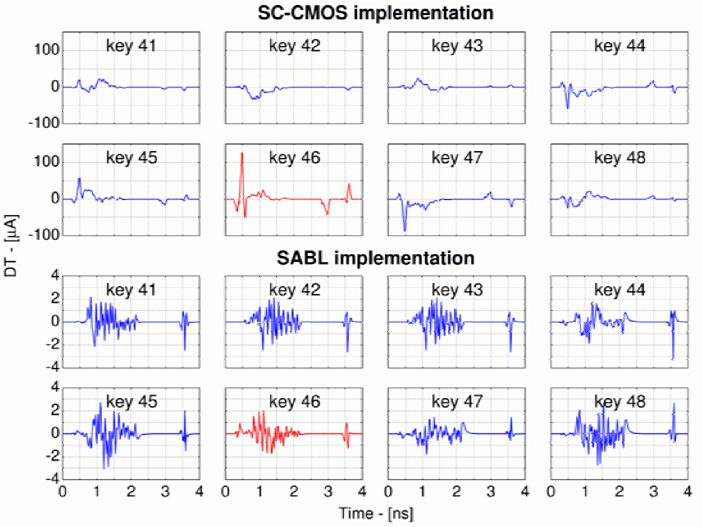
- Same circuit; two implementations.
- Difference in logic style:
  - <u>static CMOS</u>
  - <u>SABL</u>
- 0.18μm, 1.8V CMOS technology
- 5000 encryptions
- Hspice with 10ps simulation step

Supply current profile



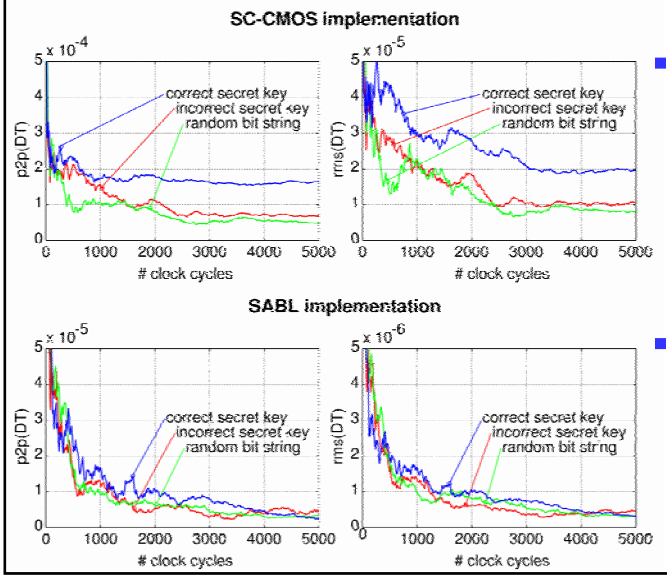
- irregular ⇒ input dependent
- regular ⇒ input independent

DPA – differential trace



- secret key stands out
- secret key does not stand out

Measurements to disclosure

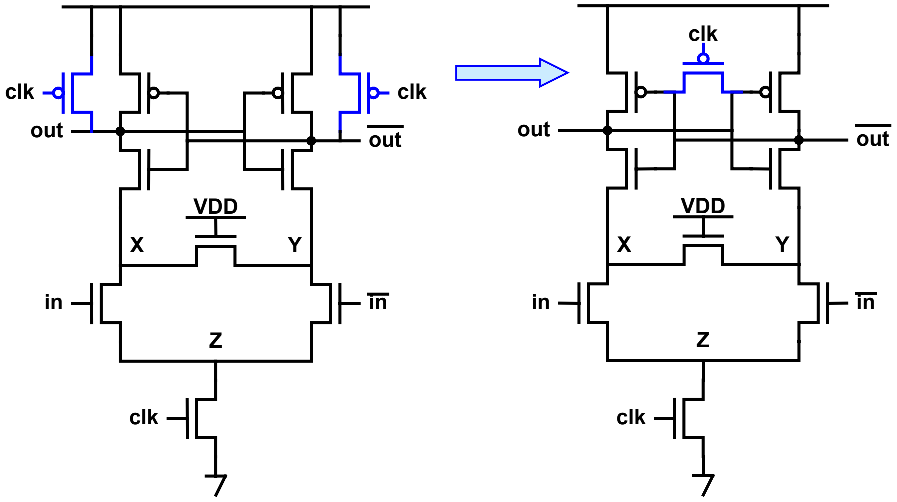


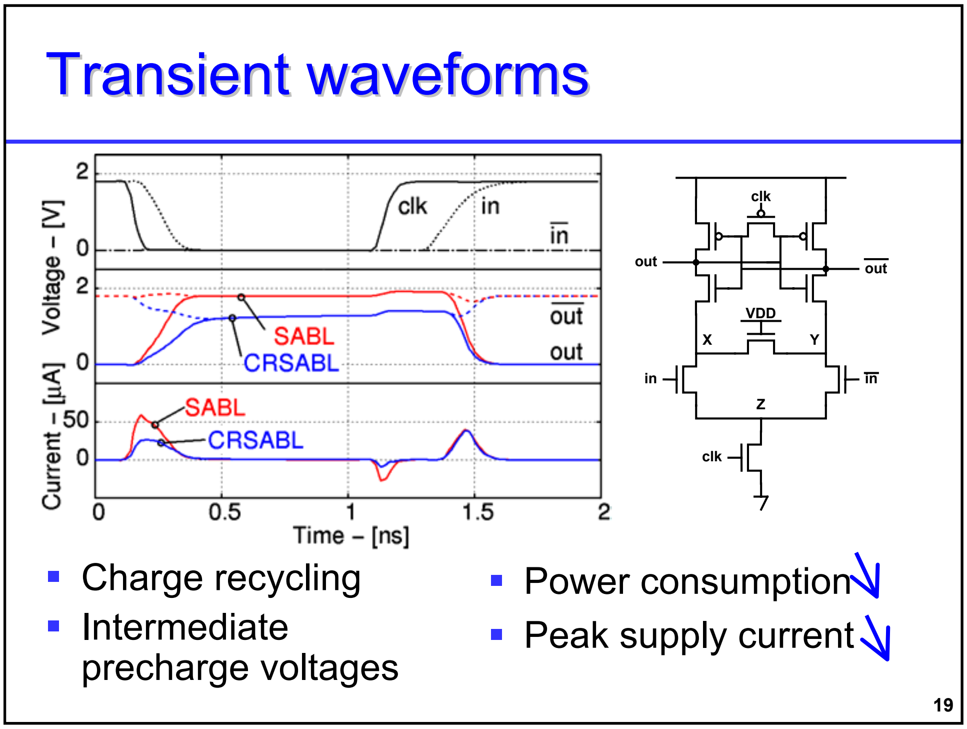
- 200 cycles sufficient to disclose key
- transient response has died out

Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions

Charge recycling SABL

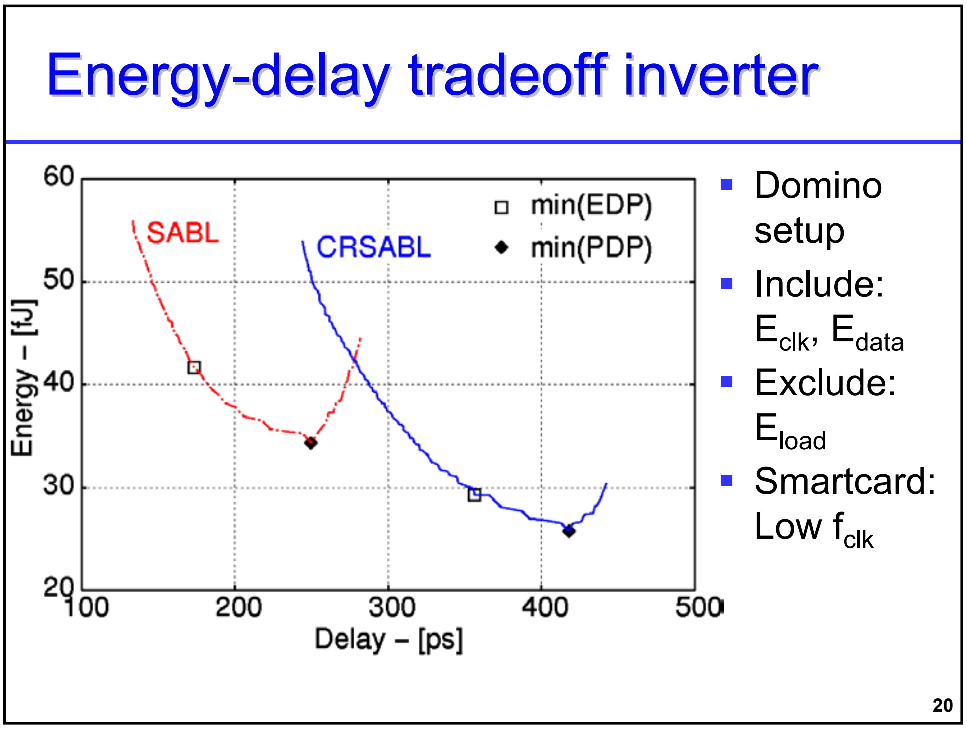




Transient waveforms

- Charge recycling
- Intermediate precharge voltages
- Power consumption ↘
- Peak supply current ↘

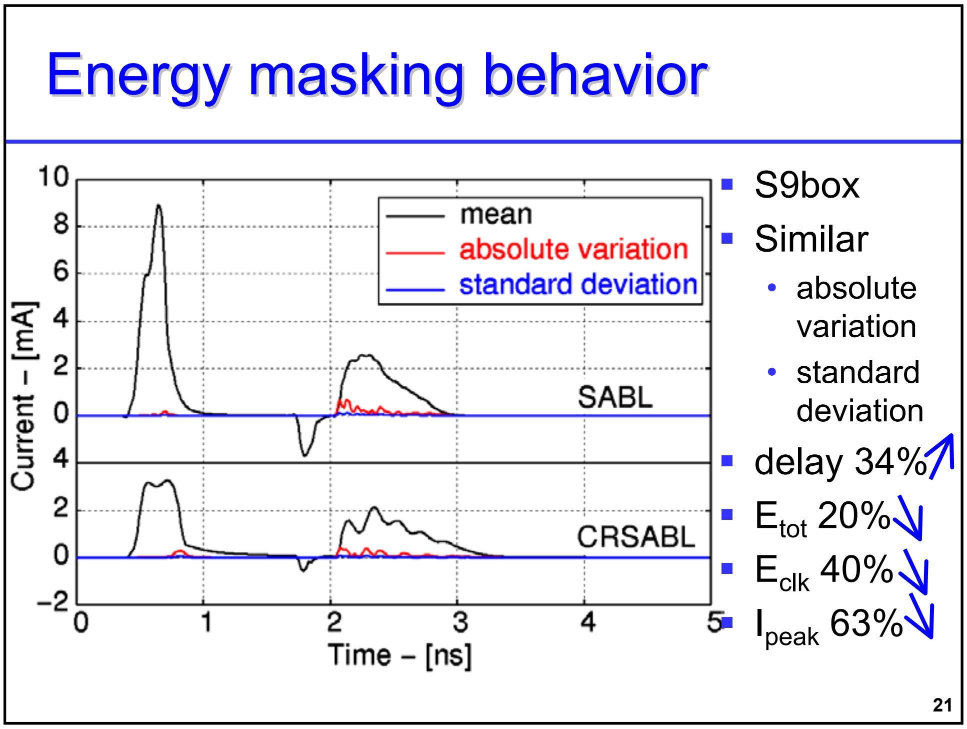
19



Energy-delay tradeoff inverter

- Domino setup
- Include: E_{clk}, E_{data}
- Exclude: E_{load}
- Smartcard: Low f_{clk}

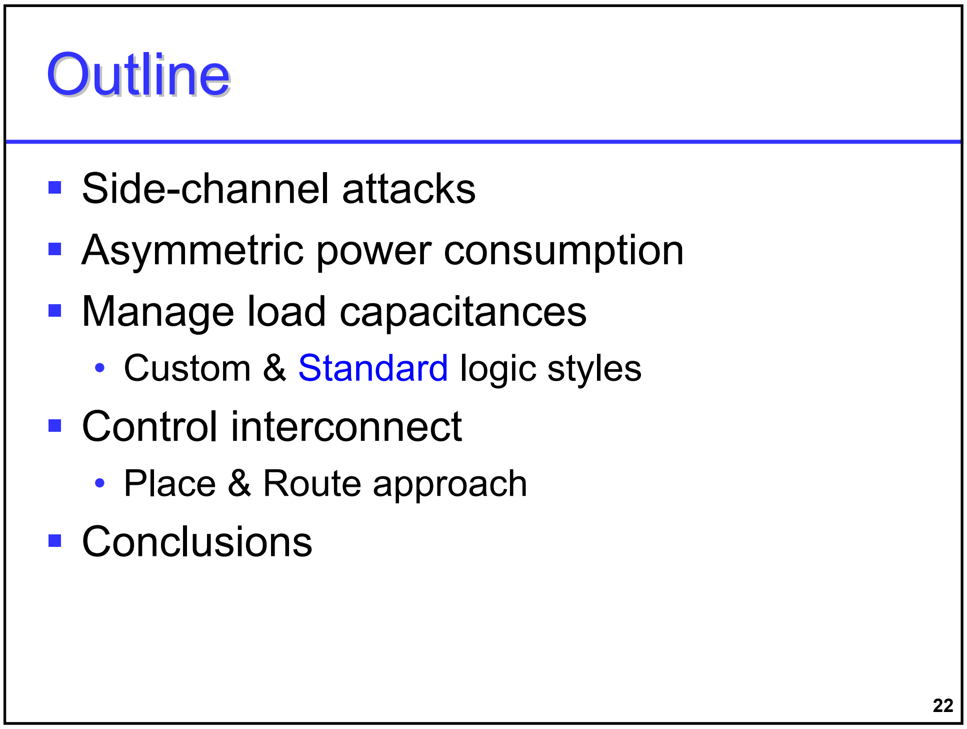
20



Energy masking behavior

- S9box
- Similar
  - absolute variation
  - standard deviation
- delay 34% ↗
- E_{tot} 20% ↘
- E_{clk} 40% ↘
- I_{peak} 63% ↘

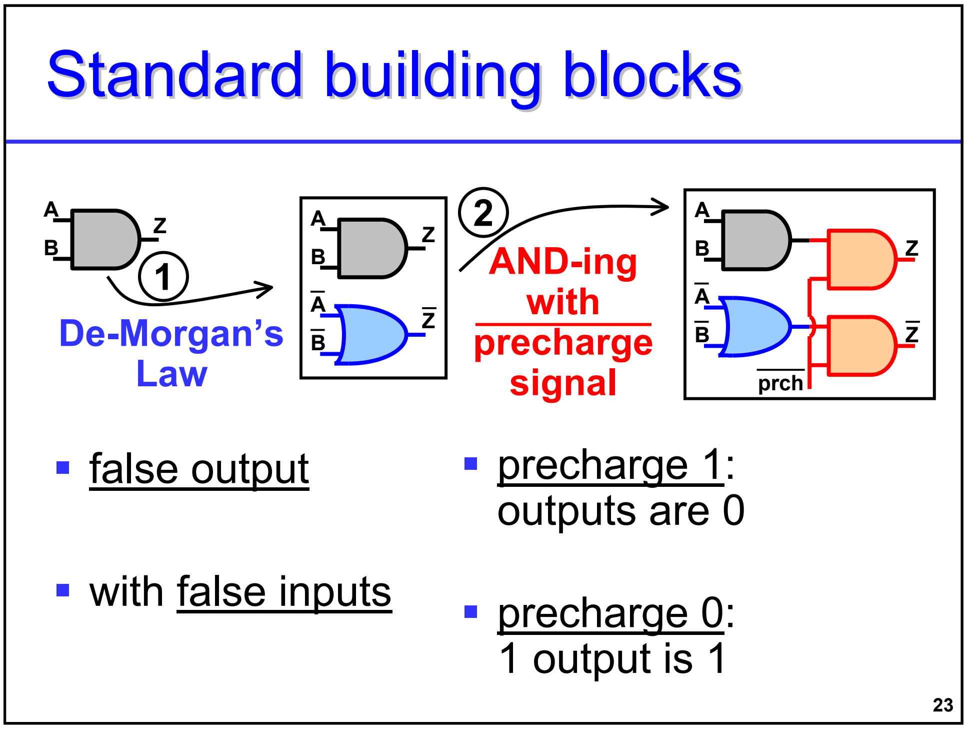
21



Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Conclusions

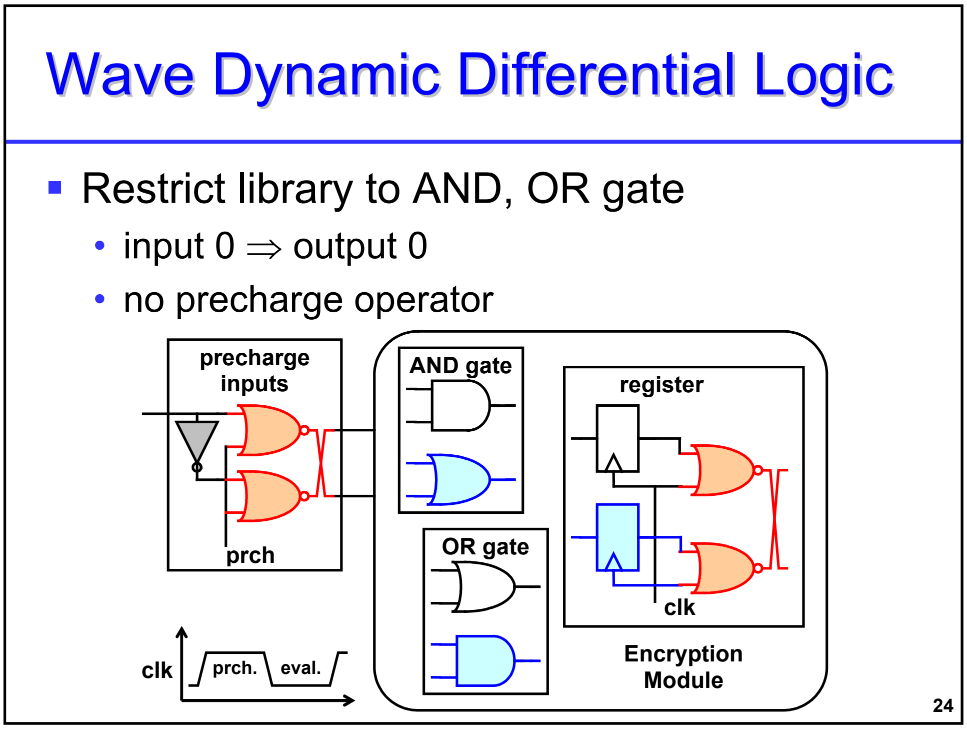
22



Standard building blocks

A
B
Z
1
De-Morgan's Law
A
B
Z
$\overline{A}$
$\overline{B}$
$\overline{Z}$
2
AND-ing with precharge signal
A
B
Z
$\overline{A}$
$\overline{B}$
$\overline{Z}$
$\overline{\text{prch}}$

- false output
- with false inputs
- precharge 1: outputs are 0
- precharge 0: 1 output is 1



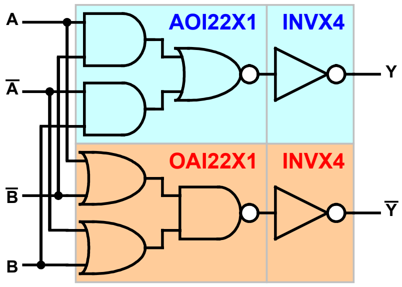
Wave Dynamic Differential Logic

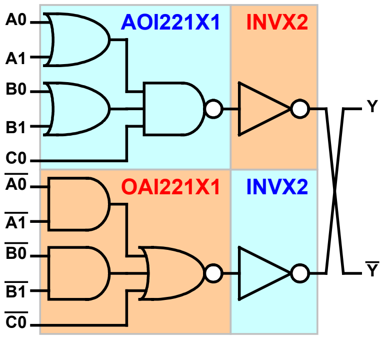
- Restrict library to AND, OR gate
  - input 0 ⇒ output 0
  - no precharge operator

precharge inputs
prch
AND gate
OR gate
register
clk
Encryption Module
clk
prch.
eval.

WDDL library

- All functions of and2, or2 operator
- In addition: inverted input, output signals
- XOR2X4: OAI221X2:



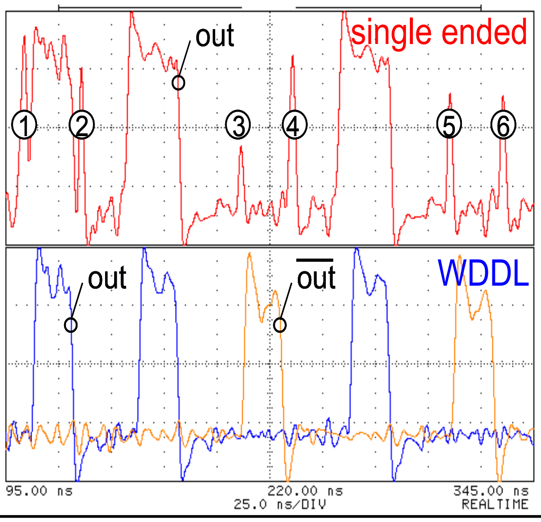


- Our WDDL library: 128 cells

25

Experimental results

- Measurement results for FPGA test circuit

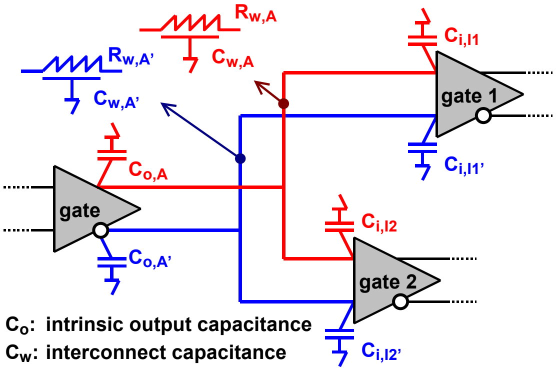


26

Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions

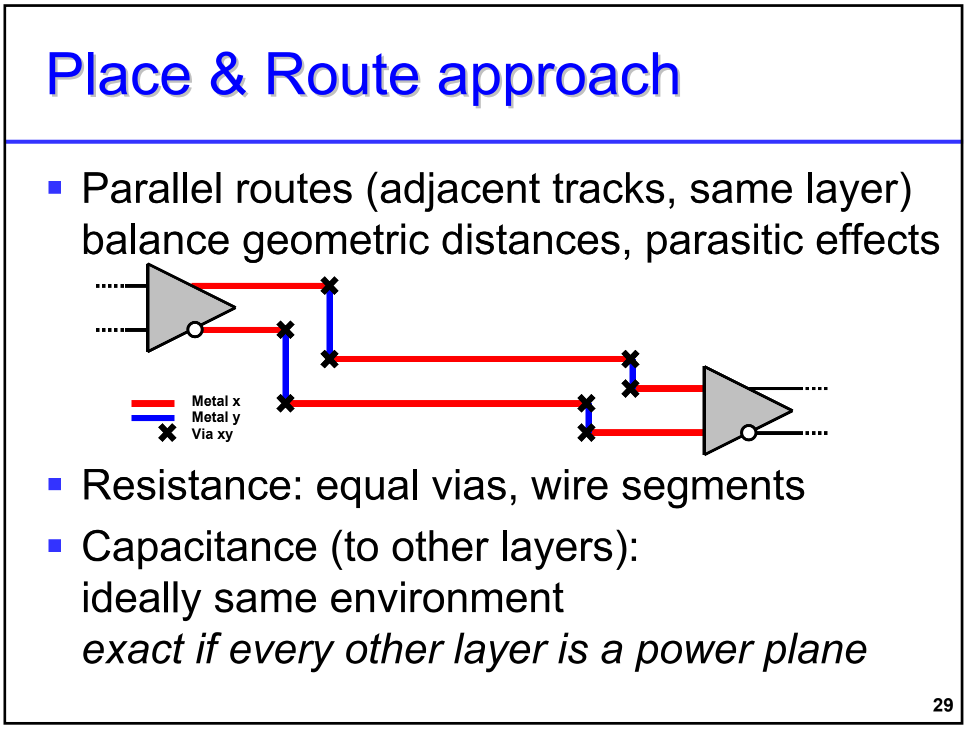
Load capacitance breakdown



C_o: intrinsic output capacitance
C_w: interconnect capacitance
C_i: input capacitance

```
              CA  = CA'
    Co,A  + Cw,A  + Ci,I1  + … Ci,Ik
=   Co,A' + Cw,A' + Ci,I1' + … Ci,Ik'
              Cw,A = Cw,A'
```

- Intrinsic caps.: matched
- Interconnect: dominant (Moore's law)
- Balancing interconnect: crucial

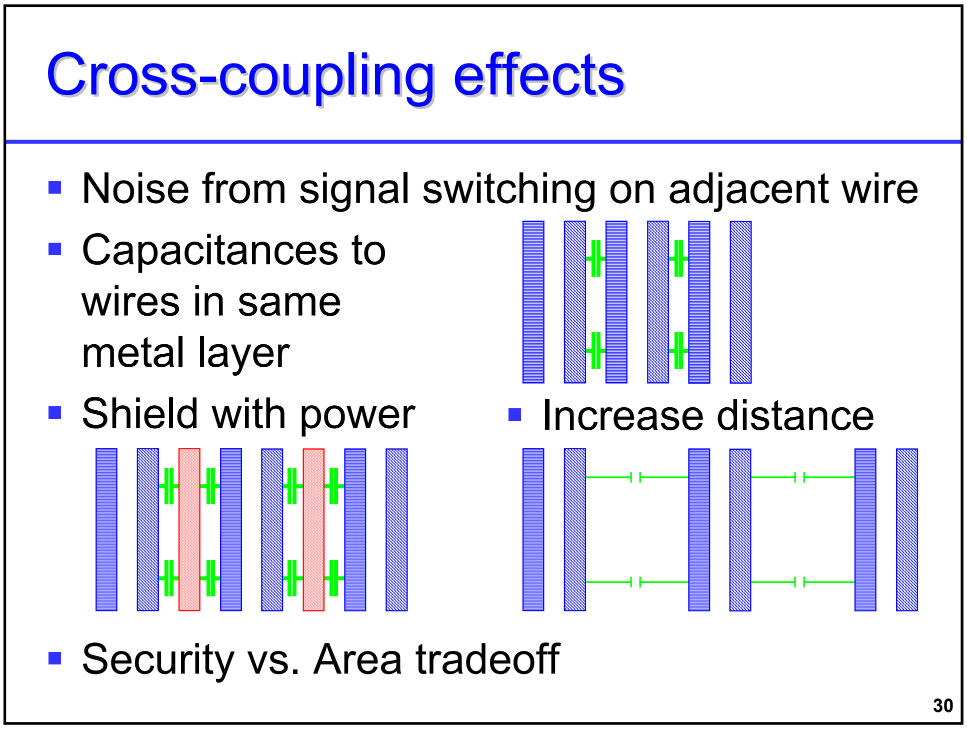


Place & Route approach

- Parallel routes (adjacent tracks, same layer) balance geometric distances, parasitic effects

- Resistance: equal vias, wire segments
- Capacitance (to other layers): ideally same environment *exact if every other layer is a power plane*

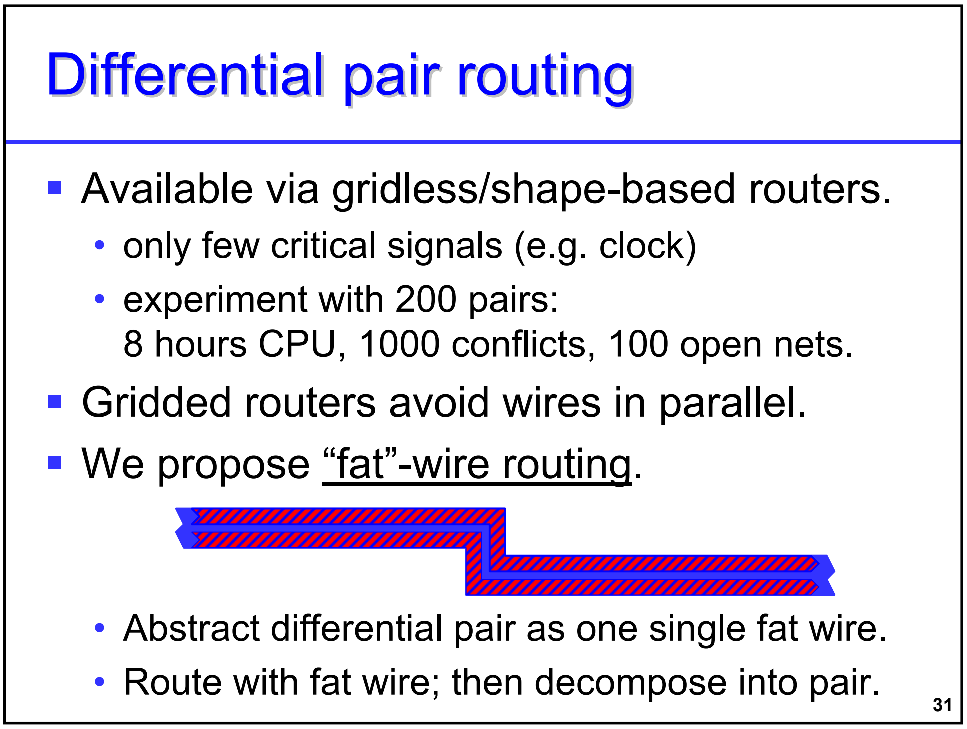
29



Cross-coupling effects

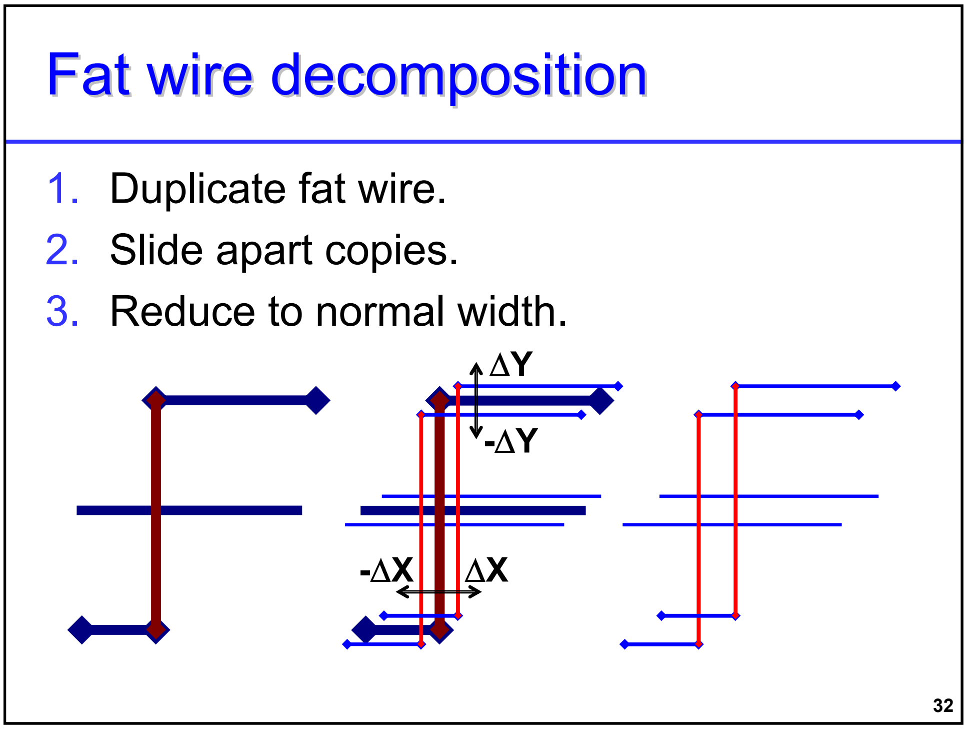
- Noise from signal switching on adjacent wire
- Capacitances to wires in same metal layer
- Shield with power
- Increase distance
- Security vs. Area tradeoff

30



Differential pair routing

- Available via gridless/shape-based routers.
  - only few critical signals (e.g. clock)
  - experiment with 200 pairs:
    8 hours CPU, 1000 conflicts, 100 open nets.
- Gridded routers avoid wires in parallel.
- We propose “fat”-wire routing.
  - Abstract differential pair as one single fat wire.
  - Route with fat wire; then decompose into pair.

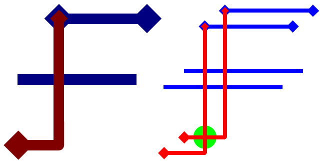


Fat wire decomposition

1. Duplicate fat wire.
2. Slide apart copies.
3. Reduce to normal width.

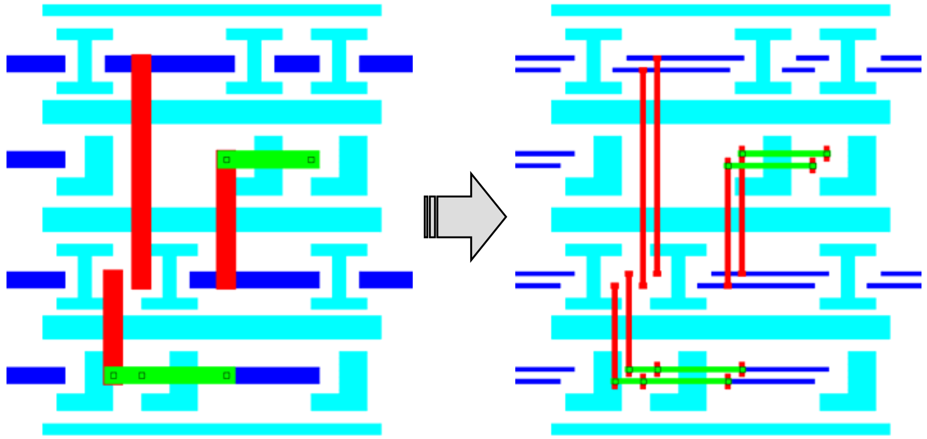
Some practical issues

- non-preferred routing:
  electric short
  if fat wire takes a turn.



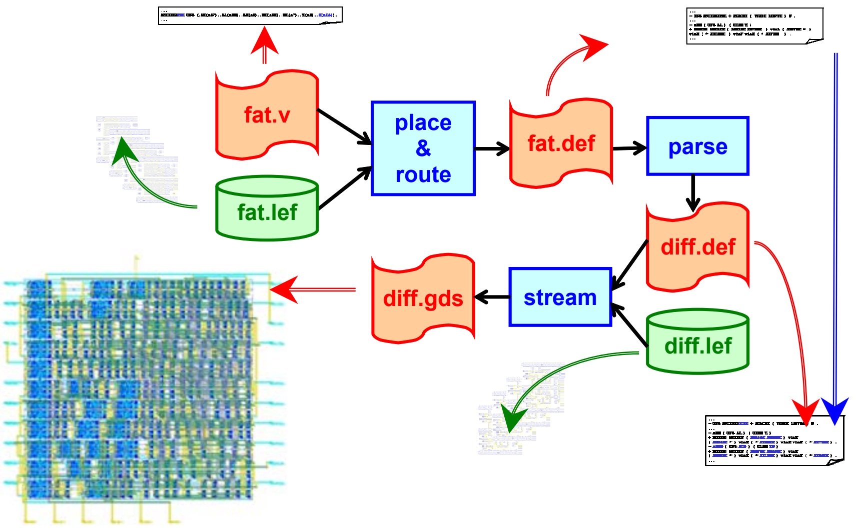
- Decomposition
  - Translation
    wire segment is defined as line between points;
    ⇨ edit these points.
  - Width reduction
    wire width is defined in the library database;
    ⇨ update the library.

Design example



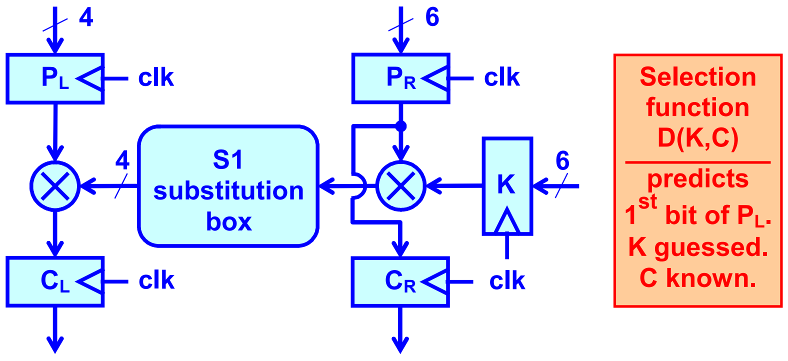
- Two normal wires replace each fat wire.

Differential routing methodology

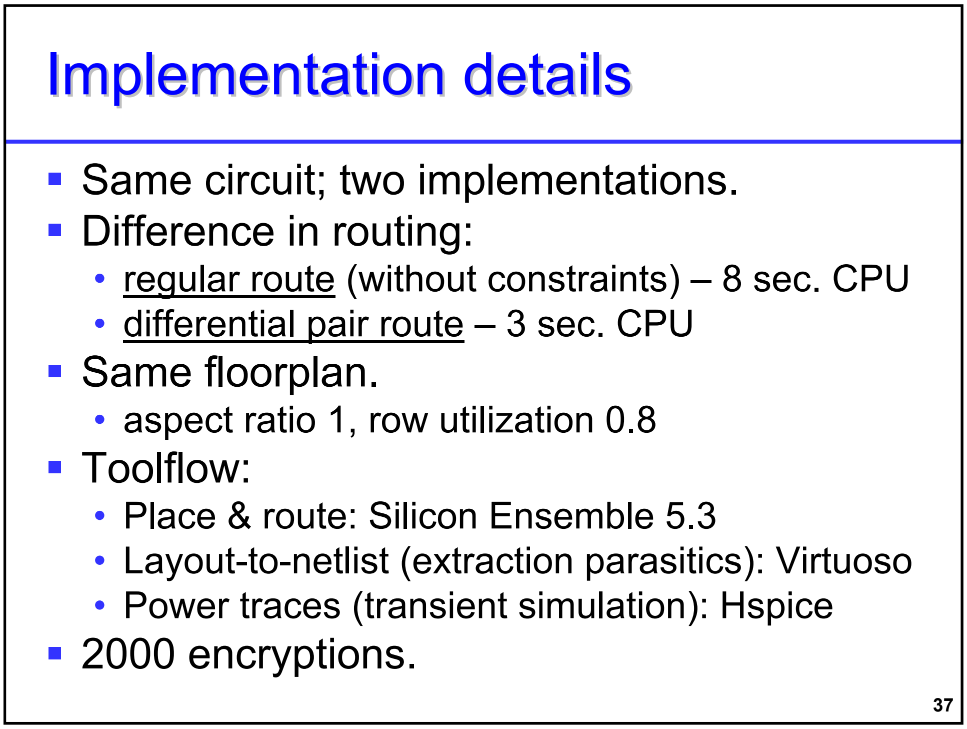


Experimental setup

- DPA on module of last round DES


4
6
P_L
clk
P_R
clk
4
S1 substitution box
K
6
C_L
clk
C_R
clk
clk
Selection function D(K,C)
predicts 1st bit of P_L. K guessed. C known.

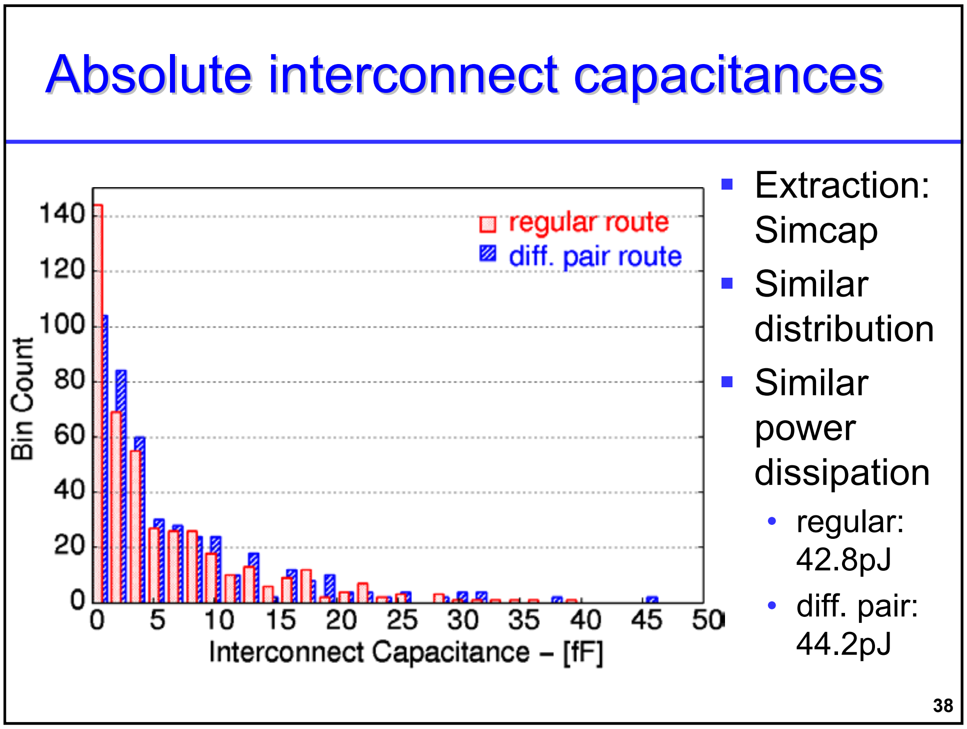
DPA: *"Power measurements are partitioned over 2 sets based on guess of secret key. Difference between typical supply currents of sets has noticeable peaks if guess was correct."*



Implementation details

- Same circuit; two implementations.
- Difference in routing:
  - regular route (without constraints) – 8 sec. CPU
  - differential pair route – 3 sec. CPU
- Same floorplan.
  - aspect ratio 1, row utilization 0.8
- Toolflow:
  - Place & route: Silicon Ensemble 5.3
  - Layout-to-netlist (extraction parasitics): Virtuoso
  - Power traces (transient simulation): Hspice
- 2000 encryptions.

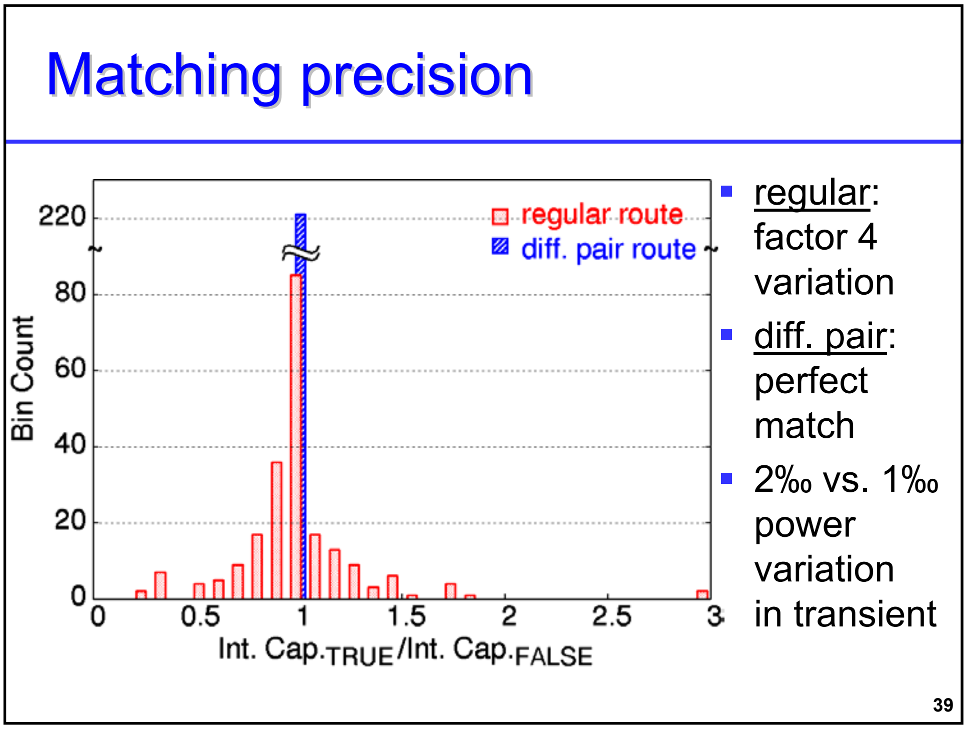
37



Absolute interconnect capacitances

- Extraction: Simcap
- Similar distribution
- Similar power dissipation
  - regular: 42.8pJ
  - diff. pair: 44.2pJ

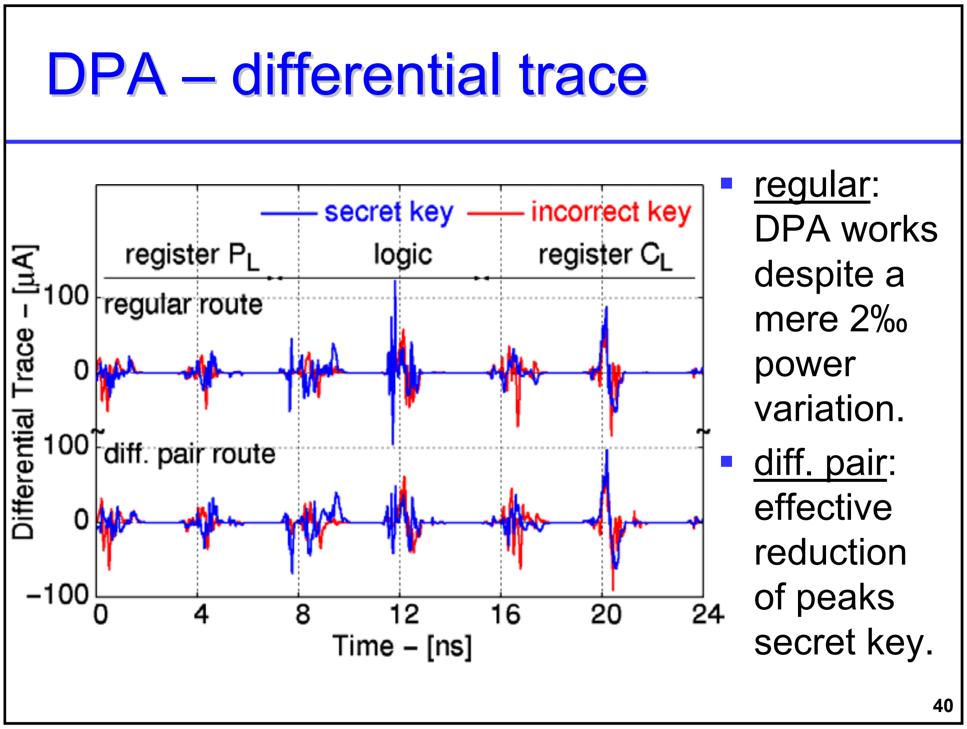
38



Matching precision

- regular: factor 4 variation
- diff. pair: perfect match
- 2‰ vs. 1‰ power variation in transient

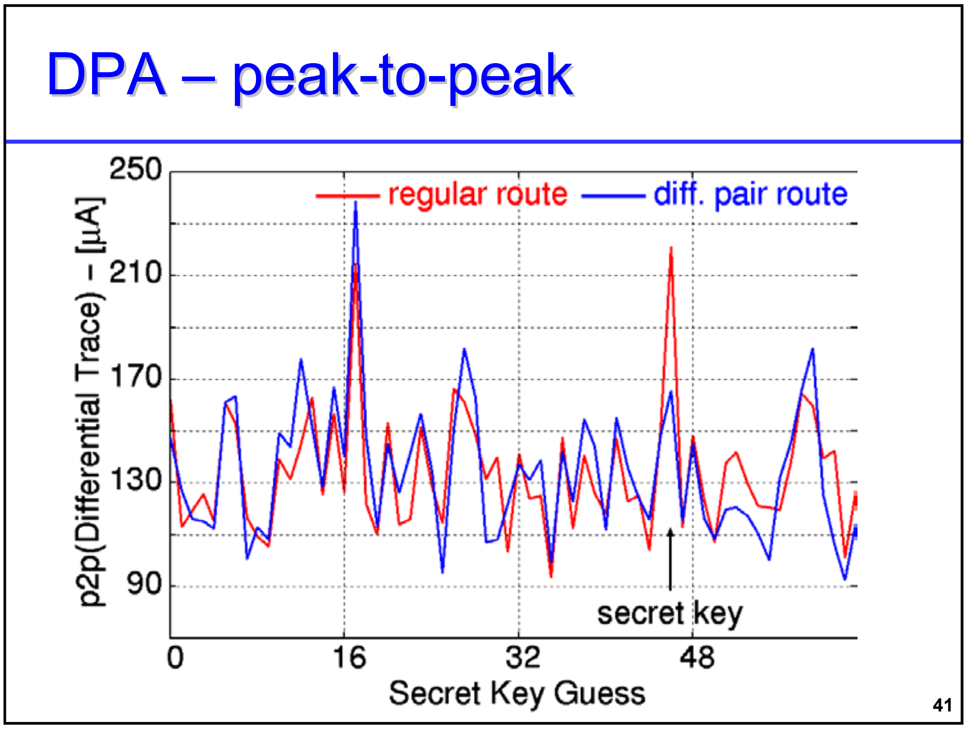
39



DPA – differential trace

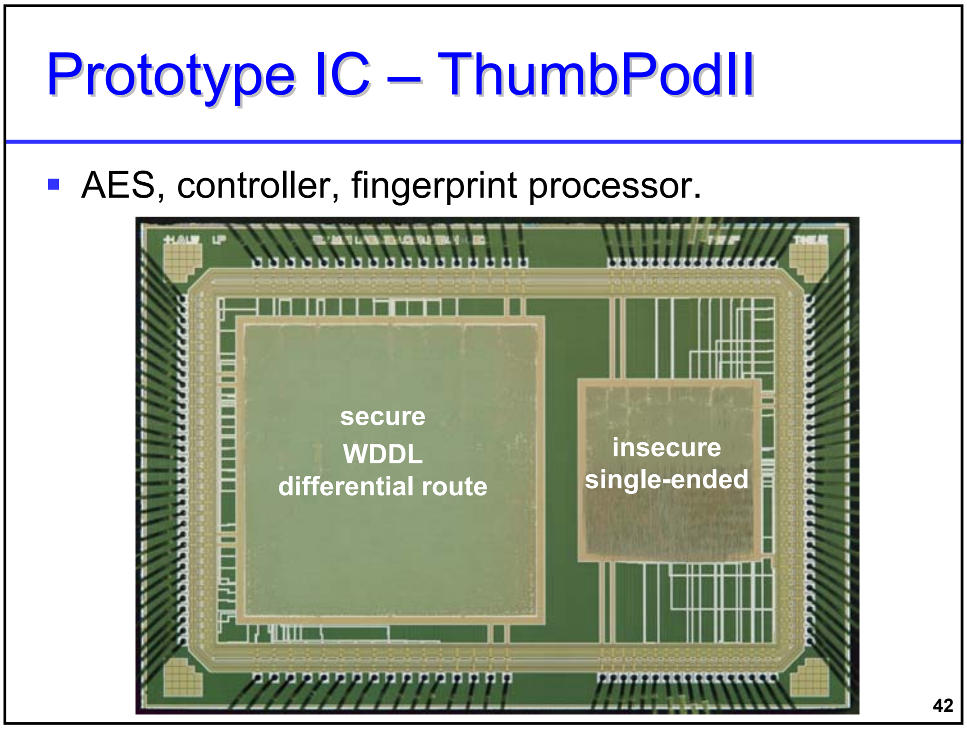
- regular: DPA works despite a mere 2‰ power variation.
- diff. pair: effective reduction of peaks secret key.

40



DPA – peak-to-peak

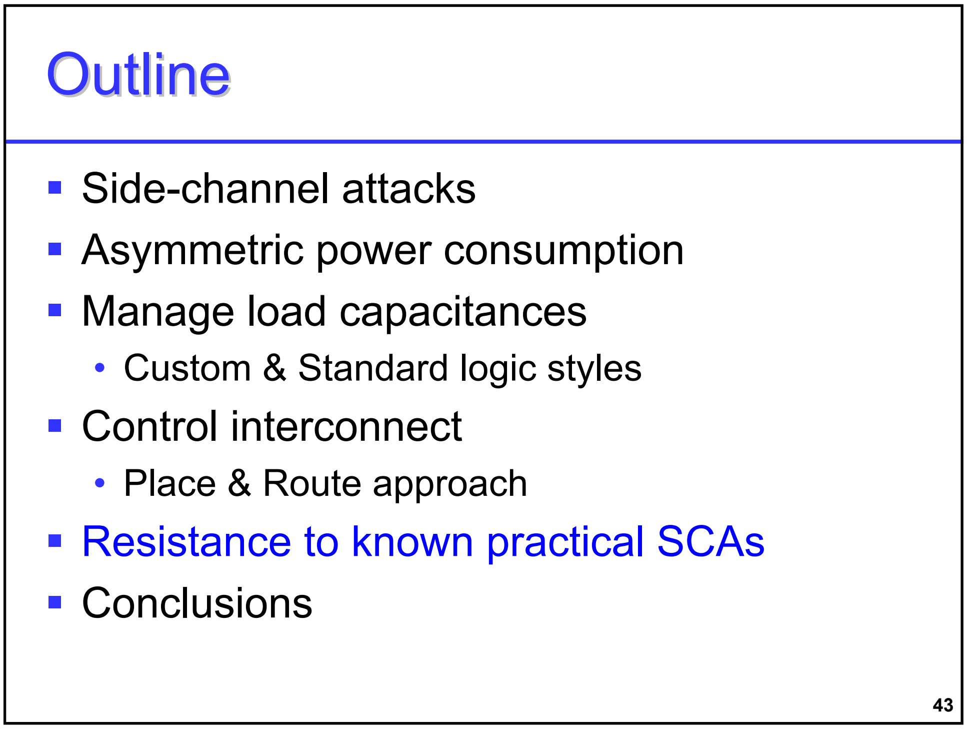
41



Prototype IC – ThumbPodII

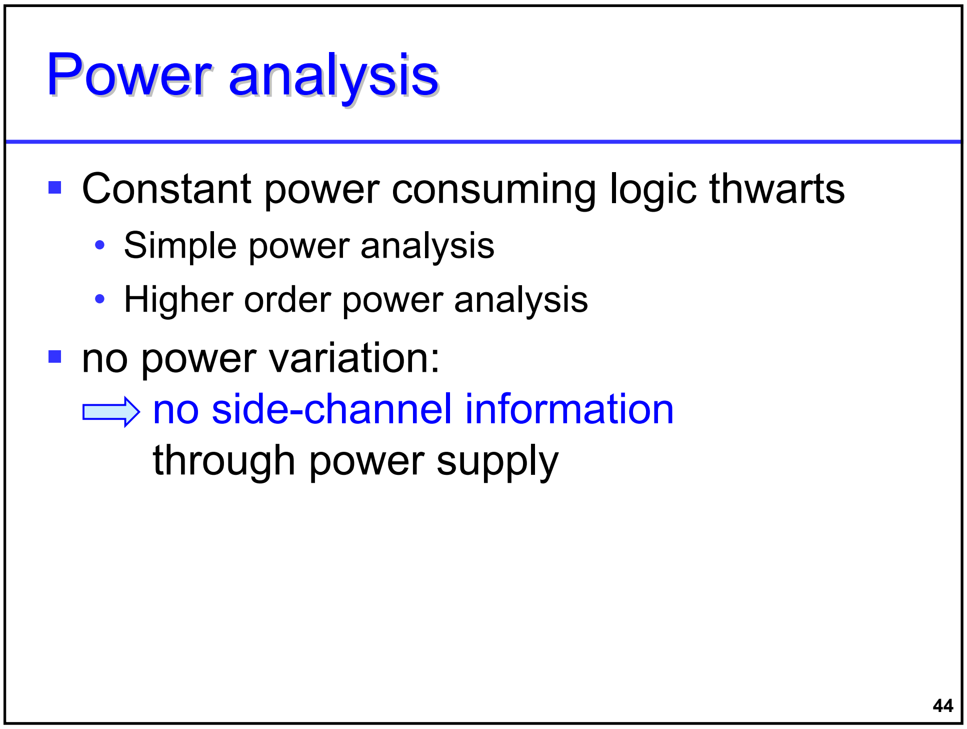
- AES, controller, fingerprint processor.

42



Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions



Power analysis

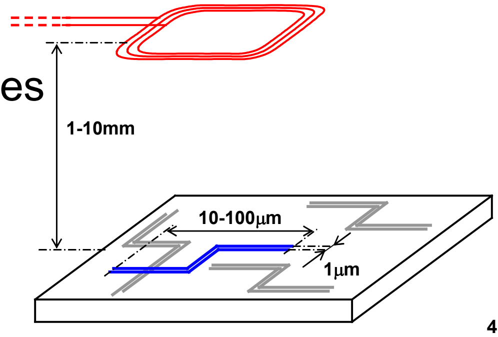
- Constant power consuming logic thwarts
  - Simple power analysis
  - Higher order power analysis
- no power variation:
  ⇨ no side-channel information
  through power supply

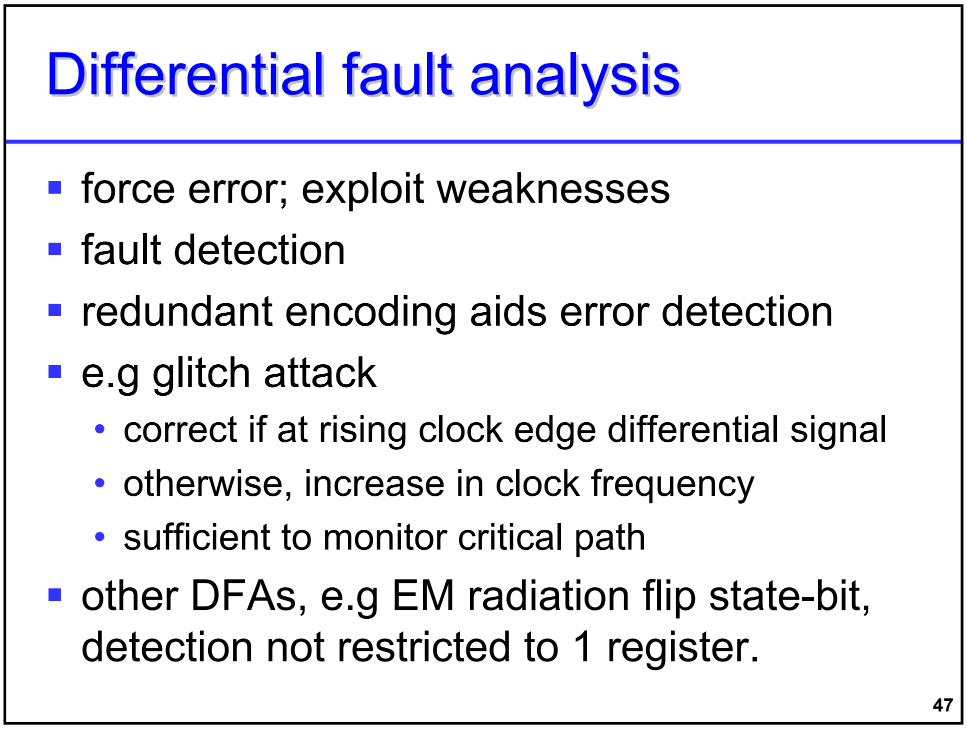
Timing attacks

- exploit timing information
- uniform power does not remove threat
- need always worst case running time
- regular logic:
  power measurements expose idle cycles
- dynamic differential logic:
  gate has a switching event in every cycle
  - whether or not useful data is processed
  - whether or not idle cycles have been inserted

Electro magnetic analysis

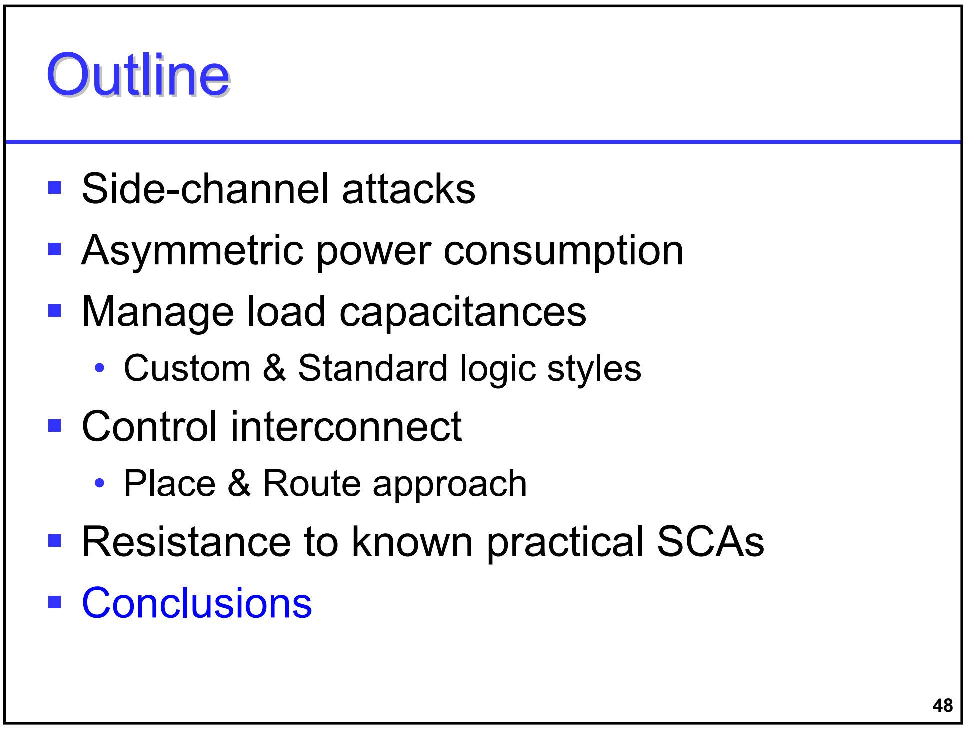
- flow of electric charges produces electromagnetic field
- can monitor small area
- ideally same
  amount of charge
  for all levels, modules
- only option: identify
  the wire





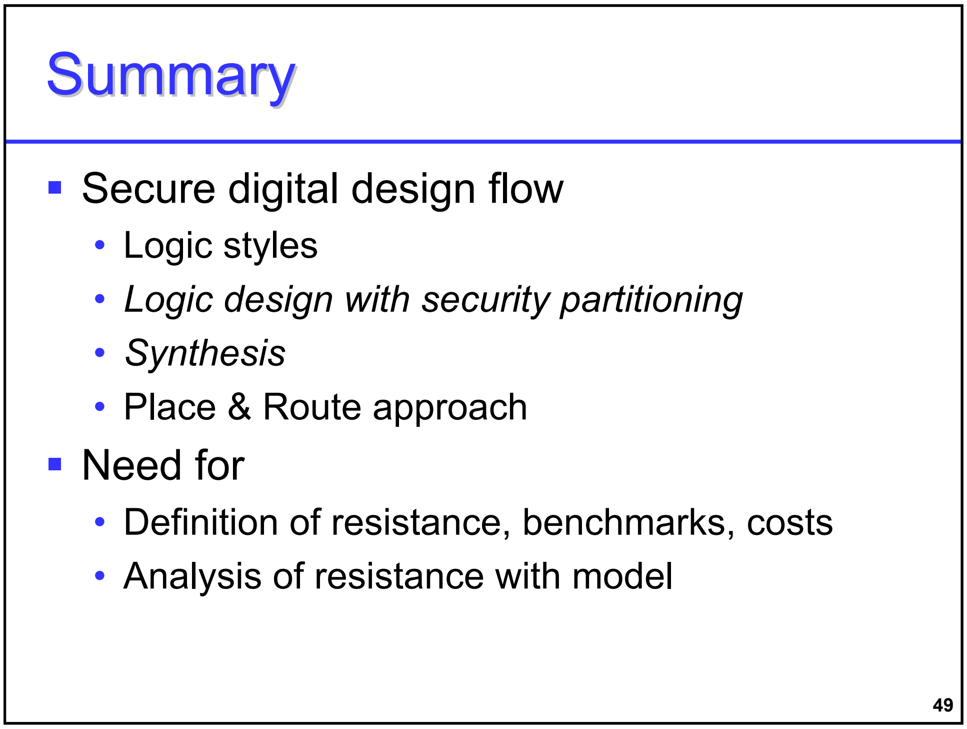
Differential fault analysis

- force error; exploit weaknesses
- fault detection
- redundant encoding aids error detection
- e.g glitch attack
  - correct if at rising clock edge differential signal
  - otherwise, increase in clock frequency
  - sufficient to monitor critical path
- other DFAs, e.g EM radiation flip state-bit, detection not restricted to 1 register.



Outline

- Side-channel attacks
- Asymmetric power consumption
- Manage load capacitances
  - Custom & Standard logic styles
- Control interconnect
  - Place & Route approach
- Resistance to known practical SCAs
- Conclusions



Summary

- Secure digital design flow
  - Logic styles
  - *Logic design with security partitioning*
  - *Synthesis*
  - Place & Route approach
- Need for
  - Definition of resistance, benchmarks, costs
  - Analysis of resistance with model