Topics of interest to CERG

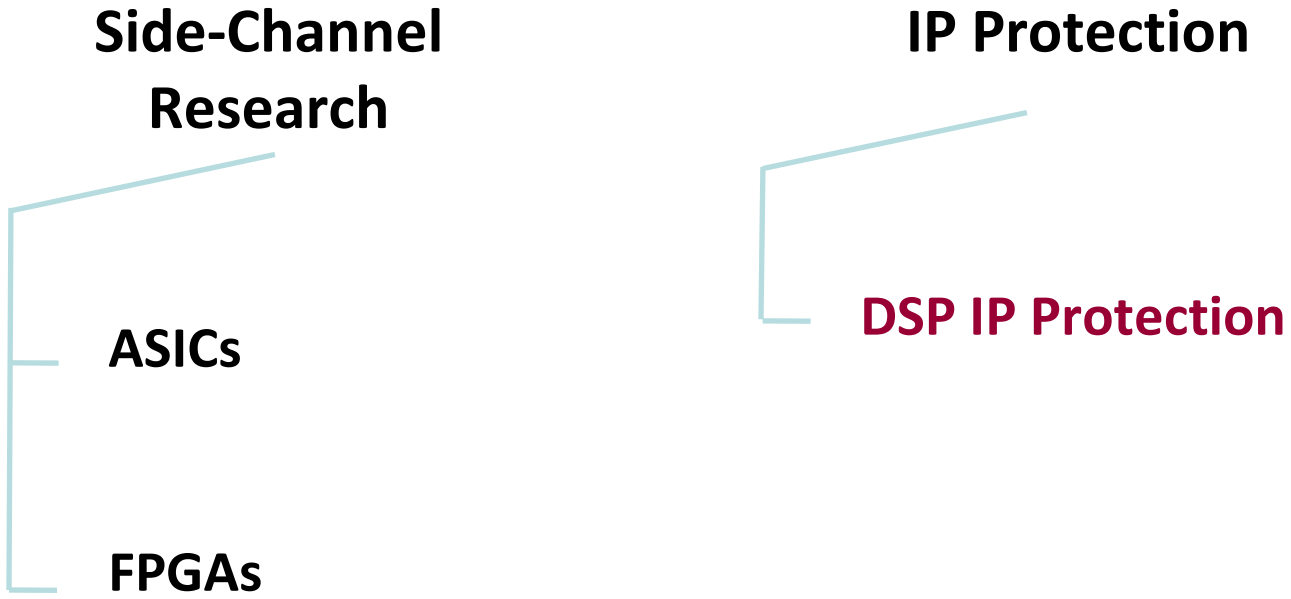
Hardware Architectures for Cryptography and Cryptanalysis

Side-channel Attacks and Countermeasures, IP Protection

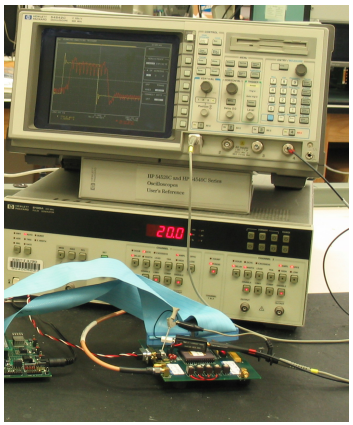
Efficient Software Implementations of Cryptologic Algorithms

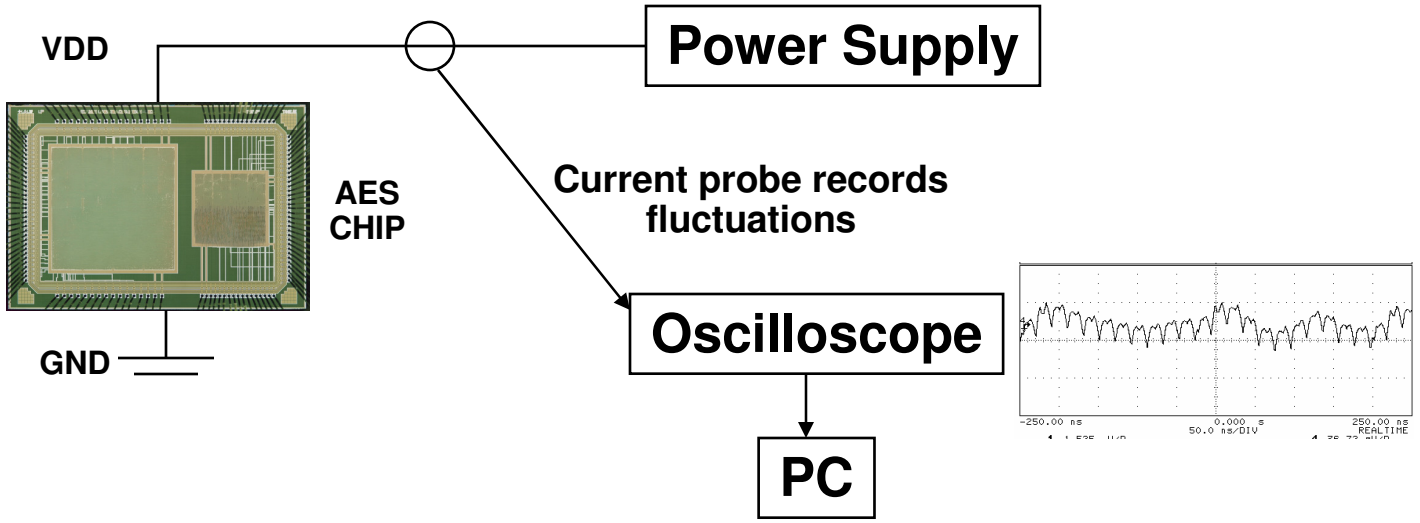
Low-power, Low-cost Cryptography for RFIDs and Sensor Networks

Side-Channel Attacks and Countermeasures, IP Protection



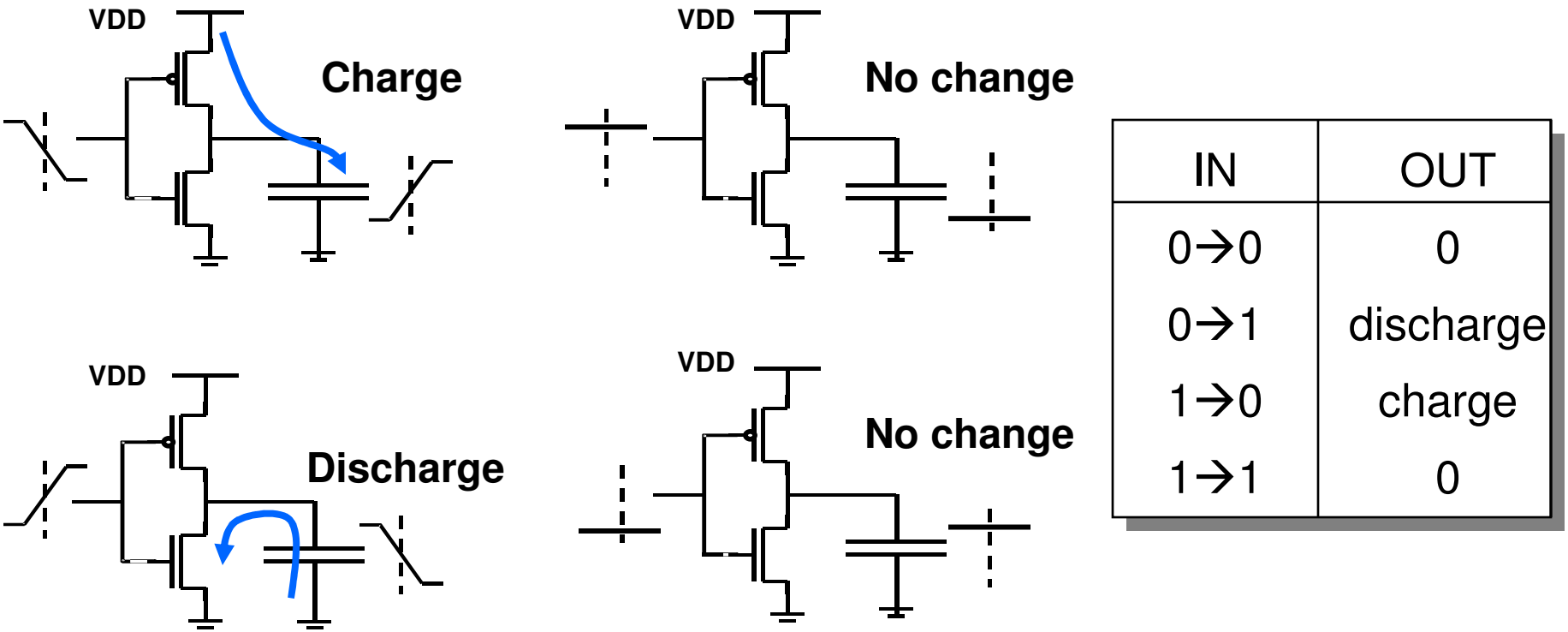
Differential Power Analysis (DPA)





- Advanced Encryption Standard (AES) with 128-bit key, brute force last longer than when Sun burns out
- DPA attack on secret key
  - Fluctuations in CMOS power dissipation reveal information about data being processed
  - Monitor power supply fluctuations via a current probe and oscilloscope
  - Perform statistical analysis in Matlab to crack the secret key
- **DPA attack on AES chip cracked in 4 minutes!**

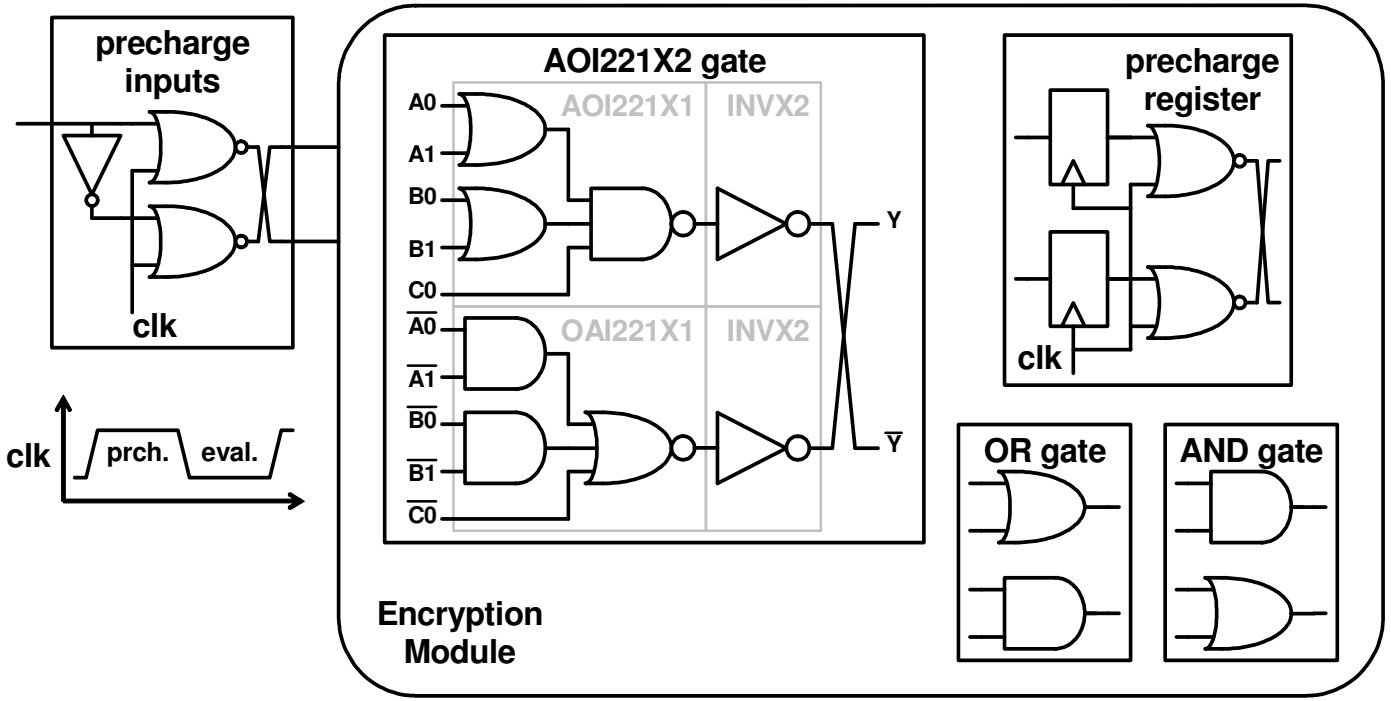
DPA: How it works



IN	OUT
0→0	0
0→1	discharge
1→0	charge
1→1	0

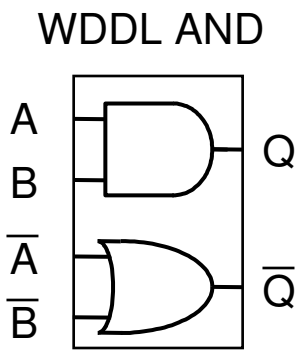
- Data-dependent asymmetry in power signature of an IC
- Exploiting asymmetry with statistical analysis, a secret key of an encryption device can be extracted
- Goal of circuit techniques: same power dissipation regardless of transition (0→0, 0→1, 1→0, 1→1), which requires two conditions:
  - Logic gate has one charging event per clock cycle: WDDL
  - Logic gate charges a constant capacitance in that cycle: differential routing

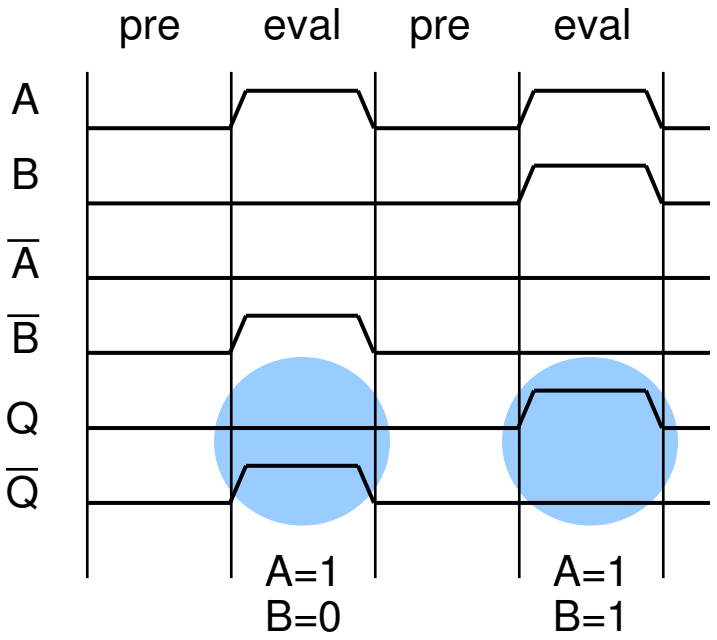
Combating DPA: Wave Dynamic Differential Logic



- Methods by Kris Tiri at UCLA
- Dynamic and dual-rail logic
- At each cycle, one power event per “gate” using standard cells
  - Precharge wave causes all gates to begin low
  - During evaluation, one output goes high, the other remains low

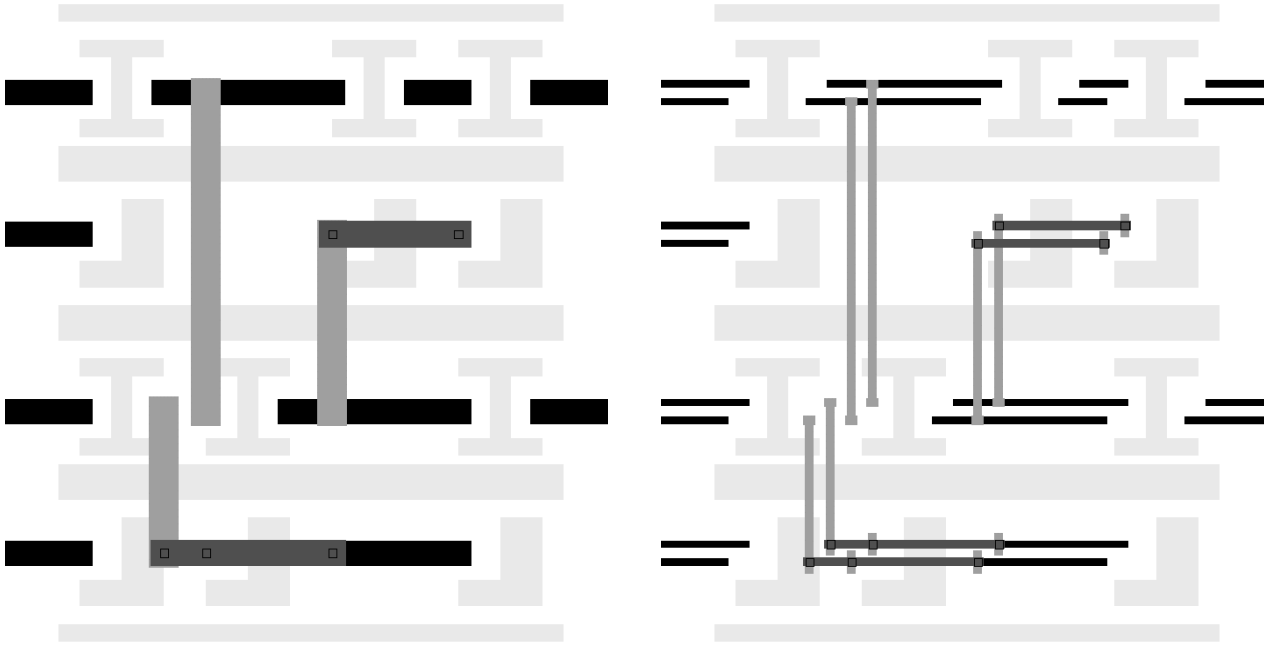
How WDDL works





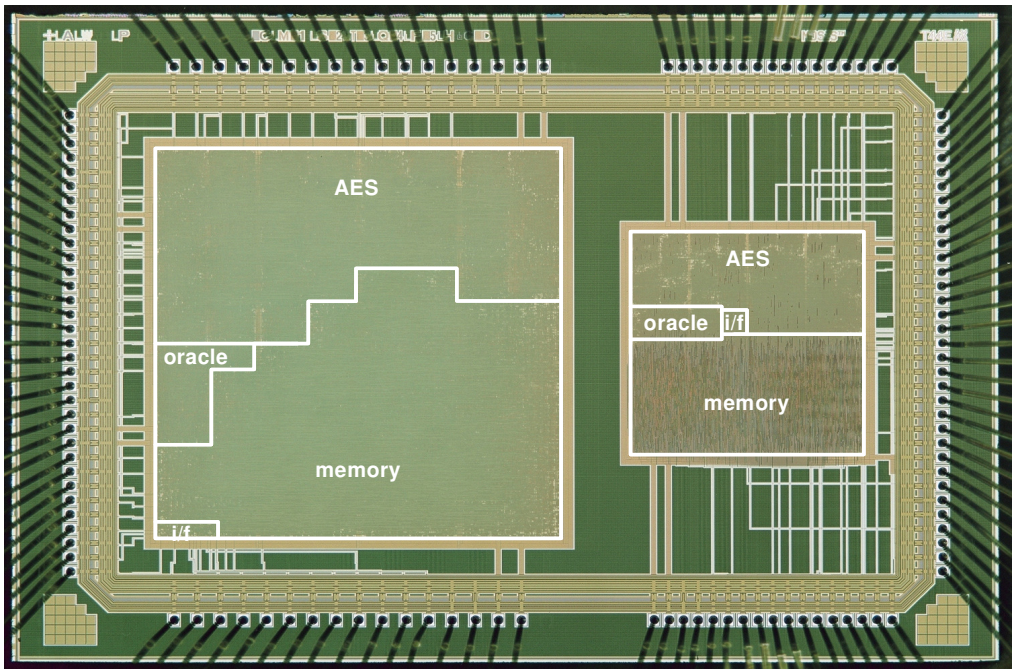
Always a single output transition

Combating DPA: Differential Routing



- True and false gates must have equal capacitance → equal power signatures
- Most capacitance in modern ICs due to interconnect capacitance, not diffusion (source/drain) or gate capacitance
- Equal interconnect capacitance: “fat” wires are routed and decomposed to parallel routes so true and false nodes have same interconnect capacitance

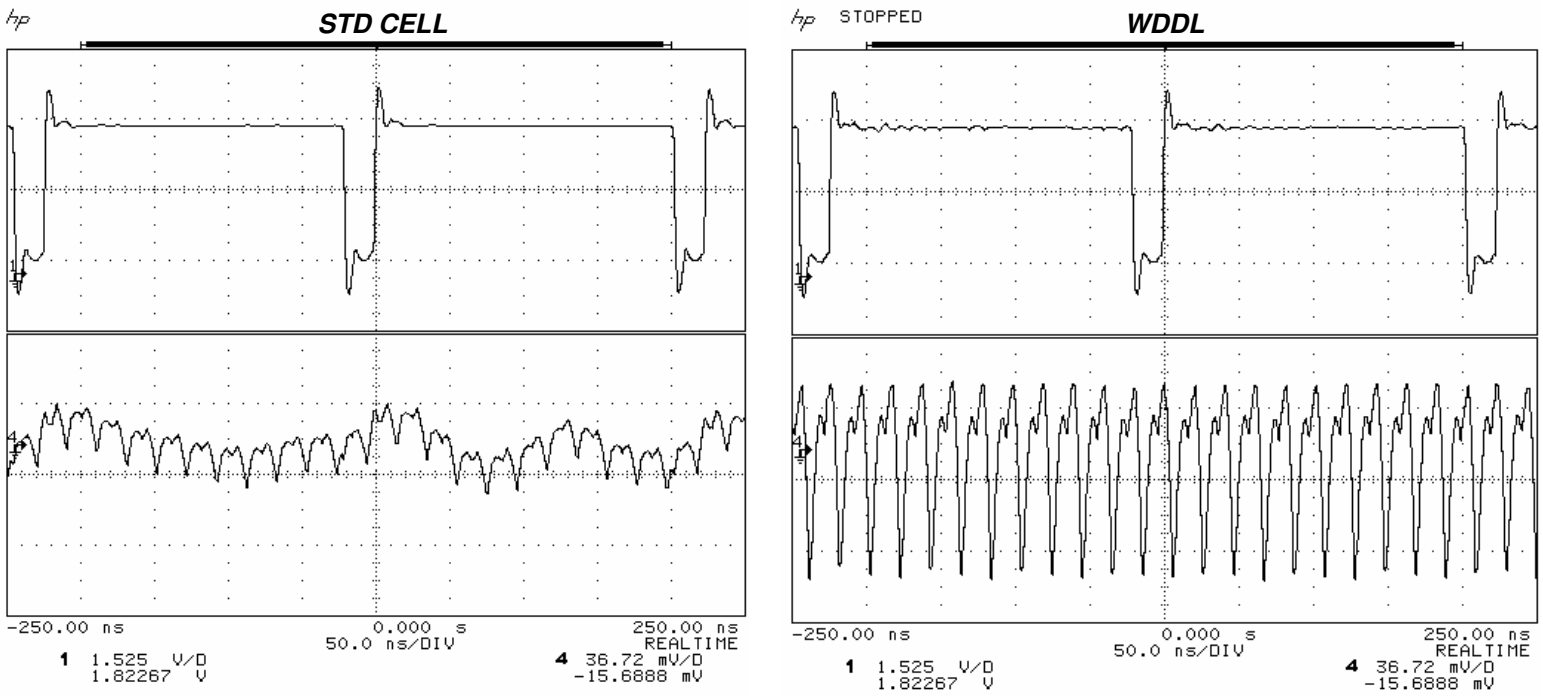
IC Micrograph



WDDL COPROCESSOR ***STD CELL COPROCESSOR***

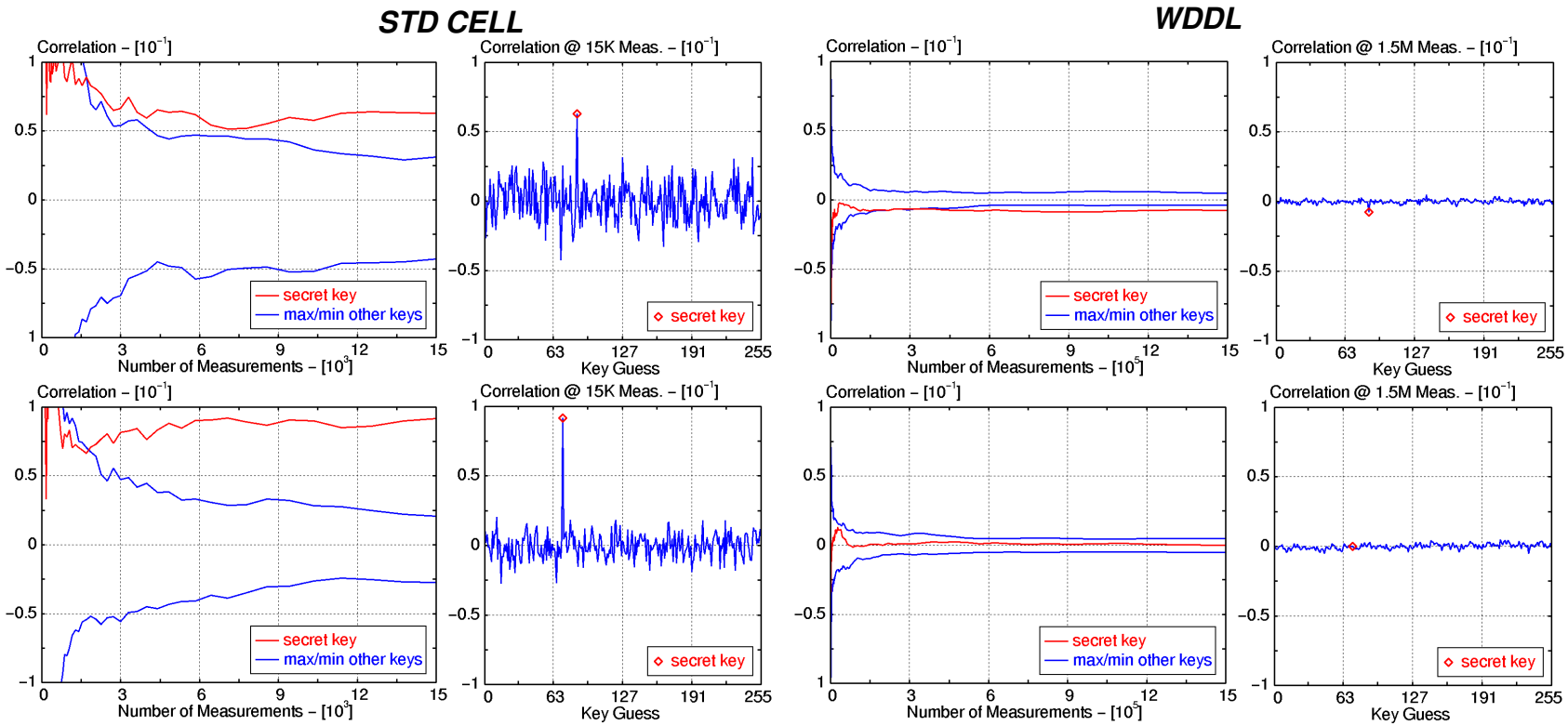
- Two functionally-identical coprocessors fabricated in 0.18-µm CMOS, 6M TSMC
  - One uses standard cells (STD CELL) and regular routing
  - One uses Wave Dynamic Digital Logic (WDDL) and differential routing

WDDL vs. STD CELL: AES Power Traces



- AES encryption start flag (top) and power supply current (bottom)
- STD CELL power variation is data-dependent → secret key easily extracted with DPA
- WDDL power variation reduces data-dependency → constant power dissipation thwarts DPA

Differential Power Analysis Results

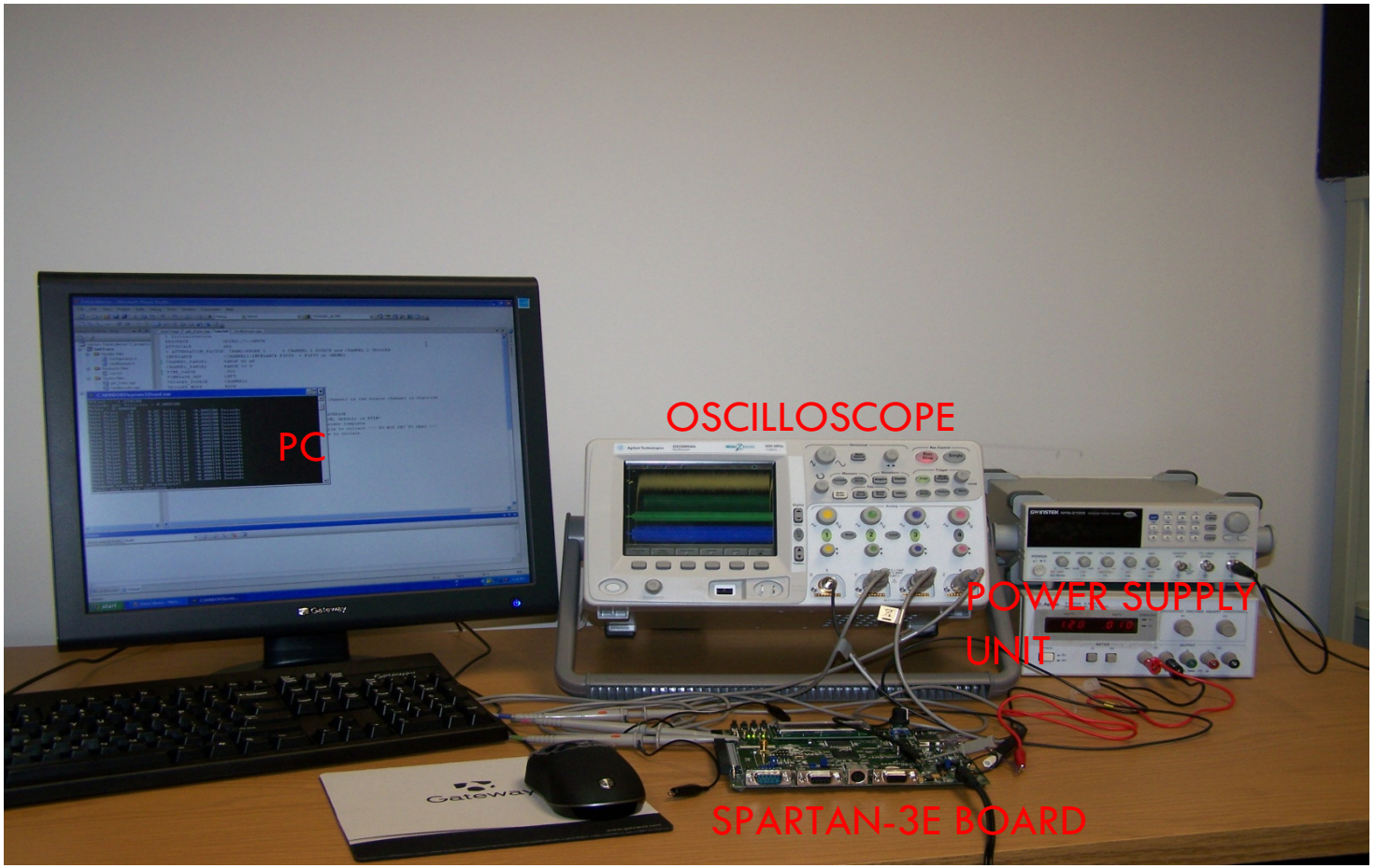


- 128 bit key is composed of 16 key bytes
- STD CELL approach, all 16 key bytes “cracked” with average of 2,000 encryption measurements (i.e. 4 minutes)
- WDDL approach, 11 bytes “cracked” with an average of 255,000 encryption measurements (i.e. 400+ minutes)
  - **Resilience to power analysis increased two orders of magnitude!**
  - **5 bytes “uncracked” after 1.5M measurements!**

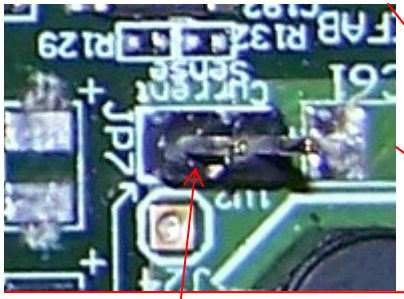
Current Research

- DPA profiling of ultra-low power implementations of lightweight symmetric-key algorithms (8-bit AES, xTEA, Camelia, etc.) to pinpoint architecture weakness
- DPA attacks and countermeasures—ciphers with heavy RAM use
- Time-based FPGA countermeasures
- Third-Party IP Protection in FPGAs

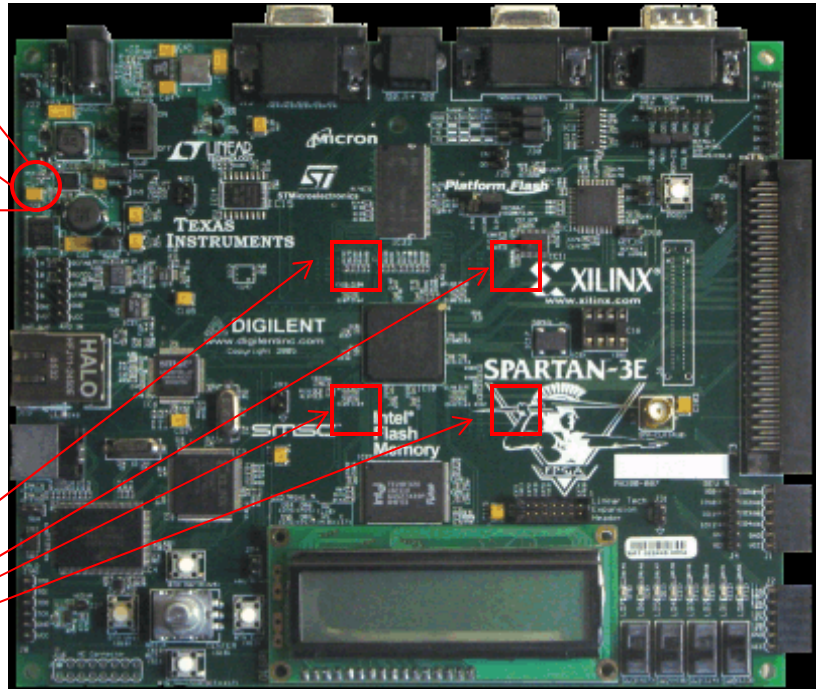
Measurement Setup



Spartan-3E board

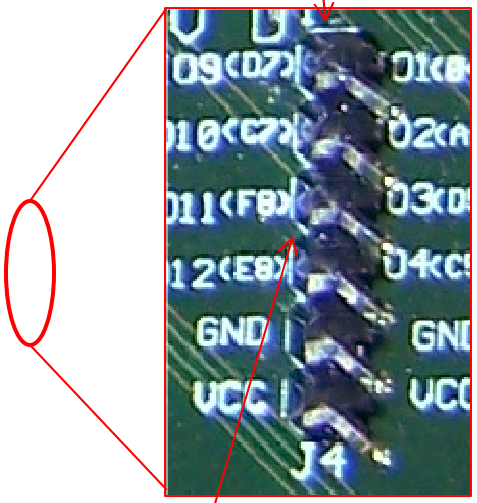


Power bypassed through this jumper



Removed Capacitors

Trigger output



Done signal

xTEA FPGA Attack

xTEA has 128 bit key and operates 64 bit block for encryption or decryption.

Has a Feistel structure.

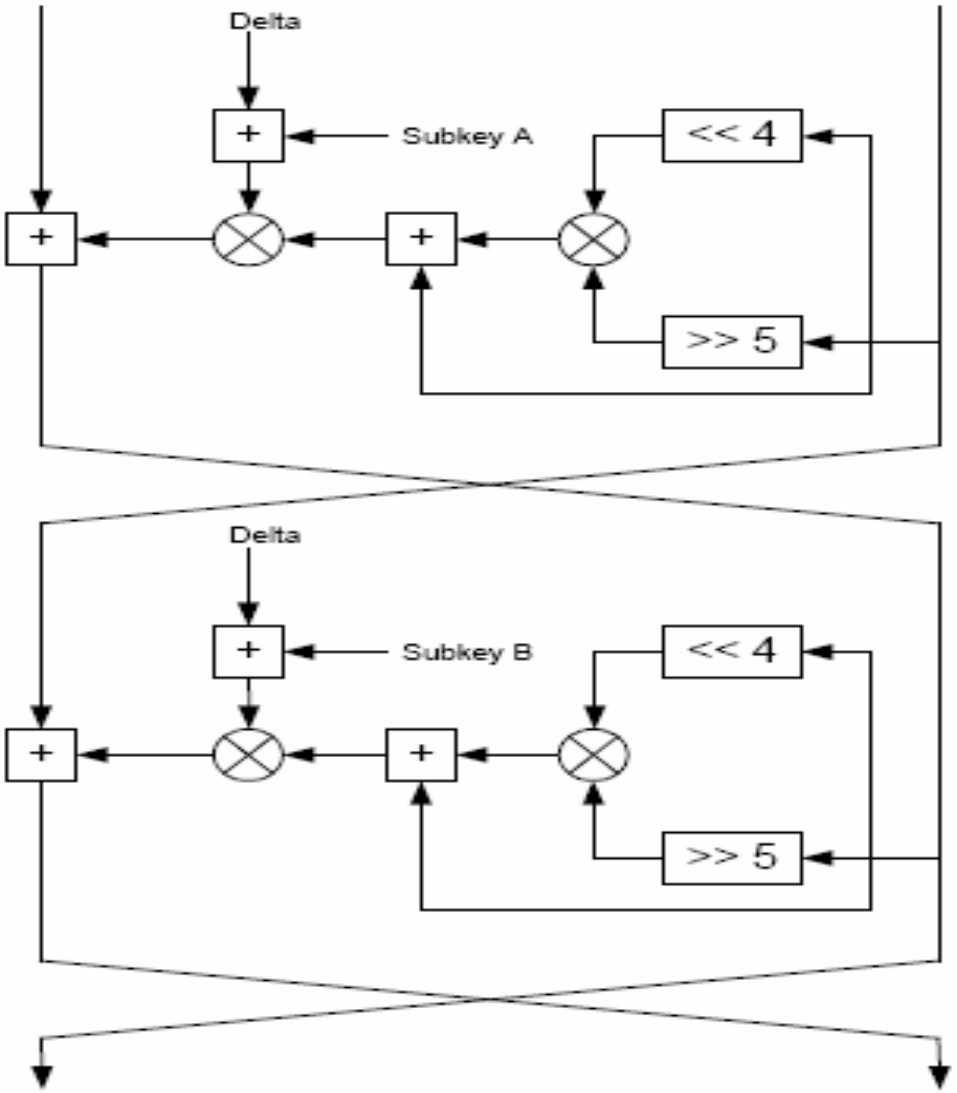
Typical number of rounds are 32.

Permutation function $f(z)=(z<<4 \ XOR \ z>>5) + z$

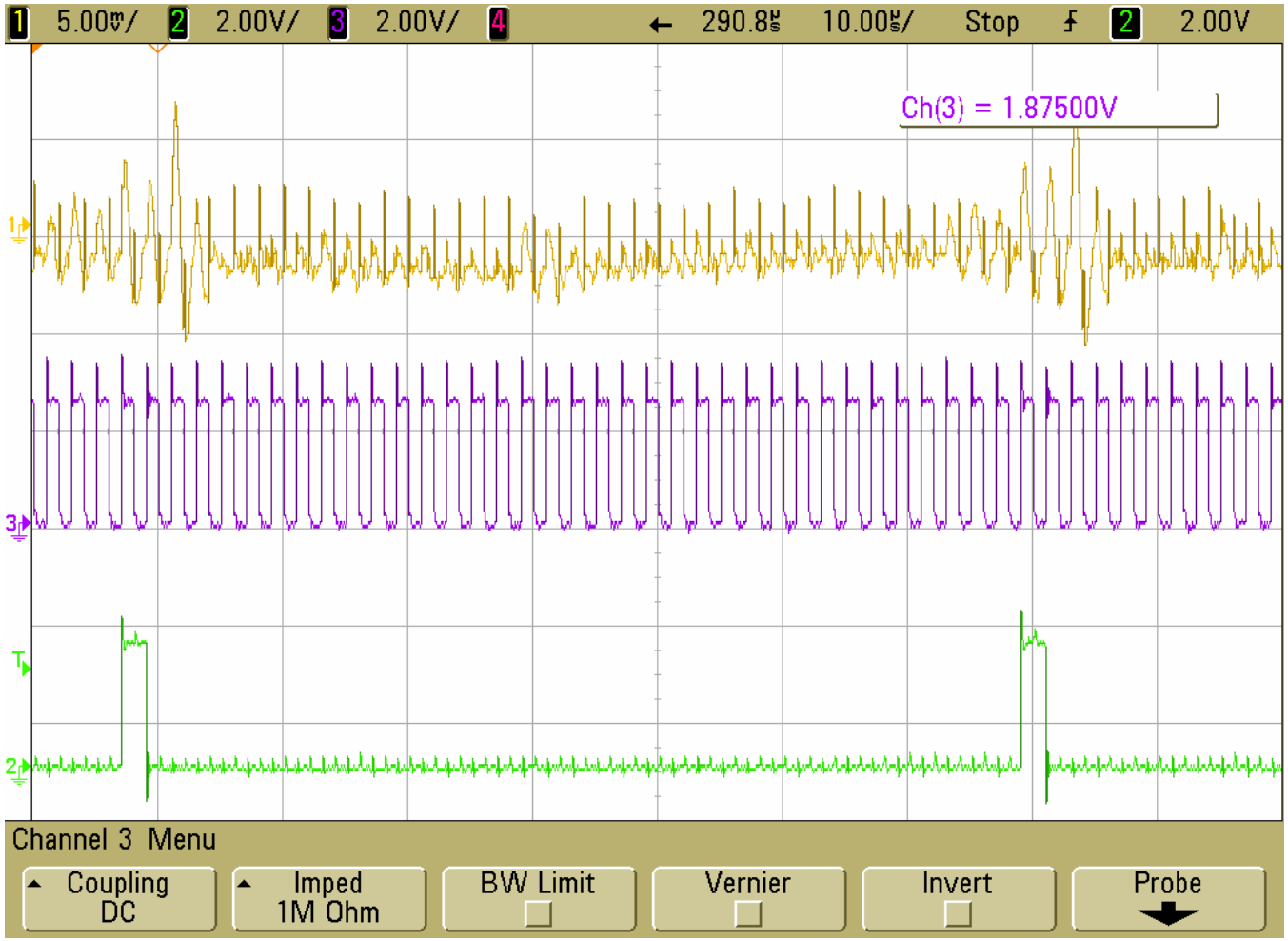
Sub key generation function $sum + k(sum)$.

Initial $sum=0$ and incremented by constant $\delta = (\sqrt{5}-1) \times 2^{31}$ between first and second half round

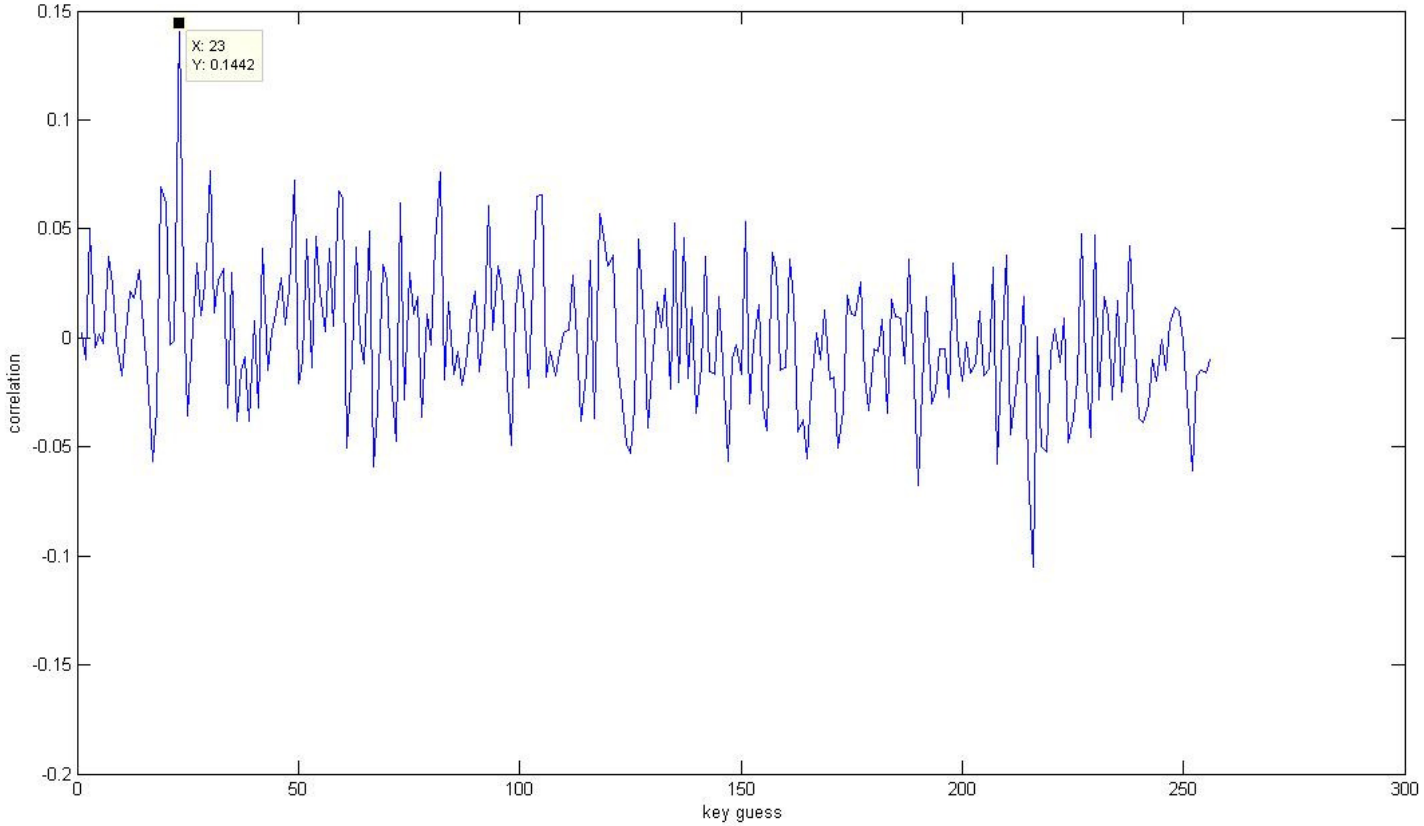
Block Diagram



Oscilloscope Waveform



Attack Results



Third-Party IP Protection

IP Provider

System Designer

- Third Party IP Provider:
  - Wants: to sell IP to system designer
  - Does not want: to lose IP before IP purchase
- System Designer
  - Wants: to purchase most efficient IP available
  - Does not want: to purchase faulty or inadequate IP