Hardware Security
-- Side Channel Attacks

Cybersecurity Specialization

What Do We Expect to Learn?

- Side channel: what, why, how, etc.
  - Cache memory
  - Power analysis (SPA, DPA)
  - Timing attacks
  - Scan chain attacks
- Countermeasures: SW, HW, Algorithm
- Background
  - Modular exponentiation, Montgomery reduction
  - Basic programming concept: assembly
  - Computer organization: memory, cache

What Is Side Channel Attack?

- Side channel attacks (SCA)
  - Monitor/measure chip's physical characteristics (power, current, timing, EM radiation, etc.) during its normal operation
  - Perform data analysis to learn information
- Features of side channel attacks
  - SCA is non-invasive and passive
  - SCA combined with other "active" methods
    - Control the normal operation via (rare) input
    - Force abnormal operation (e.g. fault injection)

Sources of Side Channel

- Measurable physical features
  - Power consumption or current
  - Timing or delay
  - Electromagnetic radiation
  - Optical
  - Acoustic
  - Output signals

Side Channel: Power and Current

- Source of power consumption
  - Dynamic power
  - Leakage current
  - Short circuit and others
- Why data may leak from power/current
  - Dynamic power: $P \propto C\ V^2\ f$
    C: effective capacitance
  - Leakage current: depend on the input vectors

Input	Leakage(*nA*)
00	37.84
01	100.30
10	95.17
11	454.50

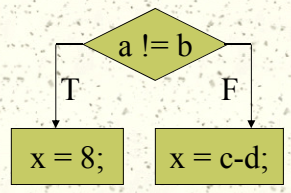
Leakage current in a 2-input NAND gate

Side Channel: Timing or Delay

- Source of timing and delay
  - Execution time required to complete an operation
- Why data may leak from timing/delay
  - Control flow
  - Data dependency
  - Cache miss
  - Pipeline stall

```
x = x * y;
y=0;
y=1;
y=64;
y =190;
```

```
if (a!=b) x=8;
else x=c-d;
```



Side Channel: EM Emission

- Source of EM emission
  - Acceleration of charges in antenna
  - Near-field (within 2 wavelength), EM waves dominate the electric and magnetic fields
  - EM wave's intensity $\propto d^{-2}$
- Why data may leak from EM emission
  - Near-field EM emissions can modulate other signals on the die.
  - EM traces can be used to reveal internal operations.

Side Channel: Optical

- Source of optical information
  - Mobile hot carries (electrons and holes) in a FET channel can cause visible or infrared light emission.
  - This can help IC testing and debug.
- Why data may leak from optical channel
  - Charge-coupled device (CCD) cameras can detect the photon emission on circuits.
  - Optical emission analysis can extract data from (smartcards, FPGAs, ASICs)

Side Channel: Acoustic

- Source of acoustic information
  - Running of on-chip components
    - Reset of key wheels of encryption engine
    - Piezoelectric effects on ceramic capacitors
  - When keyboard is hit
- Why data may leak from optical channel
  - Different trace when different key on the keyboard is hit
  - Microphone can catch the execution of RSA encryption with different key values
  - Piezoelectric effect reveals power supply information

Side Channel: Scan Chain

- Source of scan chain channel
  - On-chip registers (scan flip flops)
- Why data may leak from scan chain
  - System internal state can be read directly from scan out port during testing mode