Hardware Security -- Physical Unclonable Function (PUF)

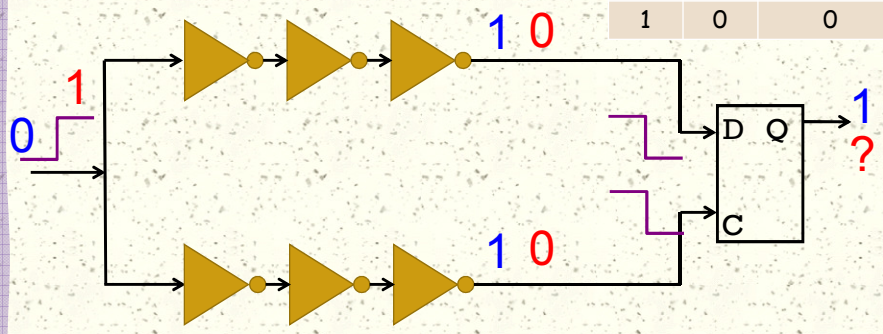
Cybersecurity Specialization

What is PUF?

- A Physical Unclonable Function (PUF) is a function that is:
  - based on a physical system
  - easy to evaluate (using the physical system)
  - behaving like a random function (that is, generating random output values)
  - unpredictable even for an attacker with physical access to the system
  - unclonable or irreproducible on another copy of the same physical system even when the functionality is known

Example

C	D	Q
0	x	No change
1	1	1
1	0	0



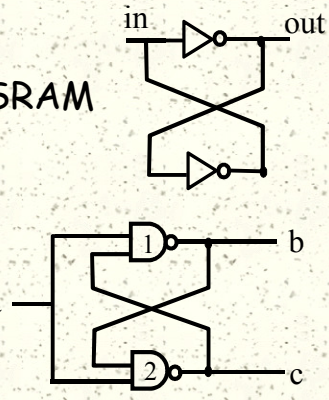
Input changes from 0 to 1: D flip flop output Q goes from 1 to 0 if the top path is faster; remains at 1 if the bottom path is faster.

Source of Physical Randomness

- Silicon PUF
  - Memory-based PUFs
  - Delay-based PUFs
  - Analog electronic PUFs
- Non-silicon PUF
  - Optical PUFs
  - Paper PUFs
  - Acoustic PUFs
  - Magnetic PUFs

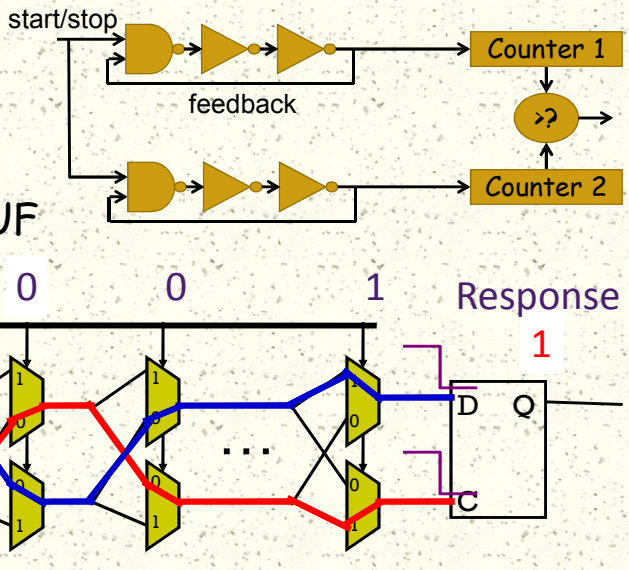
Memory-based PUF

- SRAM PUF
  - Initial power-up values of SRAM cells are random
- Latch PUF
  - Initially, a=0, b=c=1
  - Change a to 1 (metastable)
    - If gate 1 is faster, b=0, c=1
    - If gate 2 is faster, b=1, c=0
- Butterfly PUF
- Flip Flop PUF



Delay-based PUF

- RO PUF
- Arbiter PUF



Applications of PUF

- Device identification
  - The same PUF circuitry generates different (and unique) PUF data on different chips
- Key generation and storage
  - More secure than storing key in memory (e.g. physical attacks)
  - Need post-processing to make the "key" reliable, robust, and random.
- IP Protection
  - Active IC metering

Applications of PUF

- Protocols with challenge-response pairs
  - Device authentication: user has a CRP
  - Public key encryption: PUF as the secret key
- Timed authentication
  - Genuine device's response time << response time from model building attack or emulation
- Software licensing
  - PUF as the ID of the chip
- Secure memory and processor