Physical Unclonable Functions (PUF)

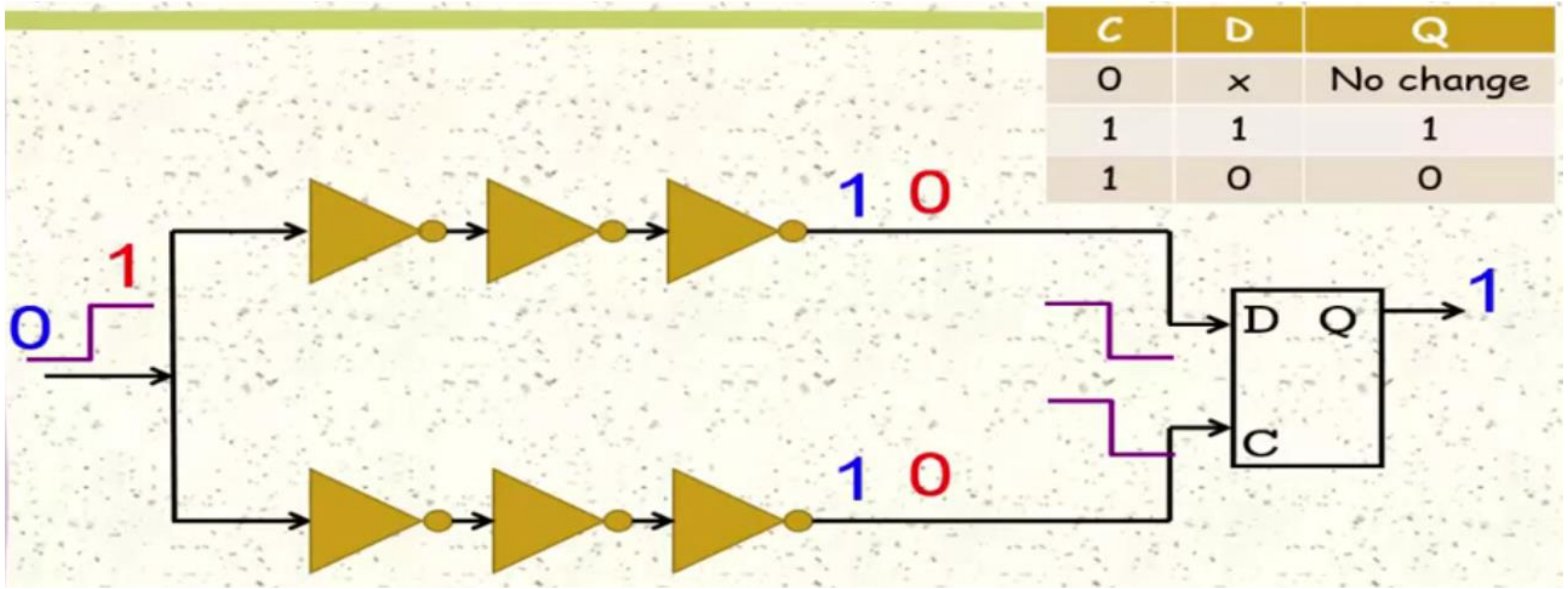
Introduction to PUFs

- Physical Unclonable Functions (PUFs) are unique hardware-based security functions. They use random physical variations in materials that occur naturally during manufacturing to create unique "fingerprints" for each device.
- The main goal of PUFs is to provide a security mechanism that relies on inherent device properties rather than software, making it more difficult to clone or replicate.
- Benefits:
  - Uniqueness
  - Non-reproducibility
  - Low Cost

How PUFs Work

- Basic Principles:
  - PUFs take advantage of inherent physical characteristics in devices due to random manufacturing variations (e.g., timing delays, material impurities).
  - When a specific input, called a "challenge," is applied to a PUF, it generates a corresponding "response." This challenge-response behavior is unique to each device.
- Example:
  - In a silicon PUF, different paths in microchips produce slight variations in timing that create unique responses when a voltage is applied.
- Key Points:
  - Responses are consistent under normal conditions but change if tampered with.
  - Ideal PUFs generate responses that are random but repeatable.

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.

Types of PUFs

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

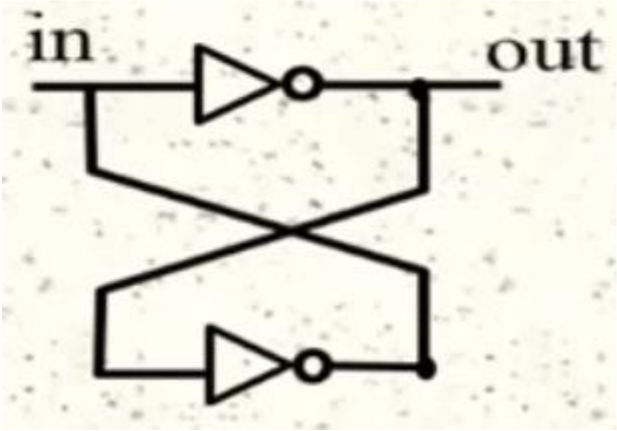
Silicon PUF

- PUFs based on silicon hardware, leveraging variations in silicon manufacturing. These are the most common and widely researched PUFs, especially for embedded systems.
- **Types of Silicon PUFs:**
  - **Memory-based PUFs:** Use unique characteristics of memory cells, such as SRAM (Static Random Access Memory) PUFs, where the power-up state of each cell is unique.
  - **Delay-based PUFs:** Utilize timing differences in signal paths on silicon to create unique signatures, such as Ring Oscillator (RO) PUFs and Arbiter PUFs.
  - **Analog Electronic PUFs:** Use analog variations in electronic components, which can vary based on environmental conditions.

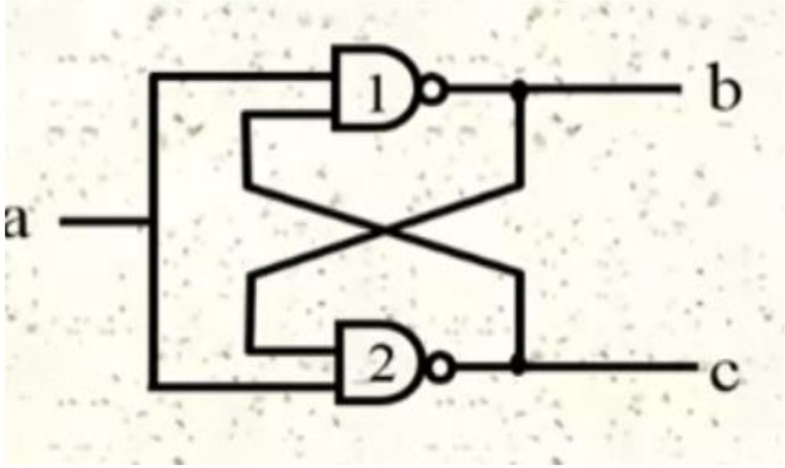
Non-Silicon PUF

- PUFs that are not based on silicon but use other physical materials and characteristics to create uniqueness.
- **Types of Non-Silicon PUFs:**
- **Optical PUFs:** Rely on light patterns reflected or scattered by a material with random microstructures, commonly used for tamper resistance.
- **Paper PUFs:** Use the random fiber structure in paper as a unique signature, useful in document authentication and anti-counterfeiting.
- **Acoustic PUFs:** Use sound waves and their unique reflections or absorption patterns through a medium to create unique identifiers.

Memory-based PUF

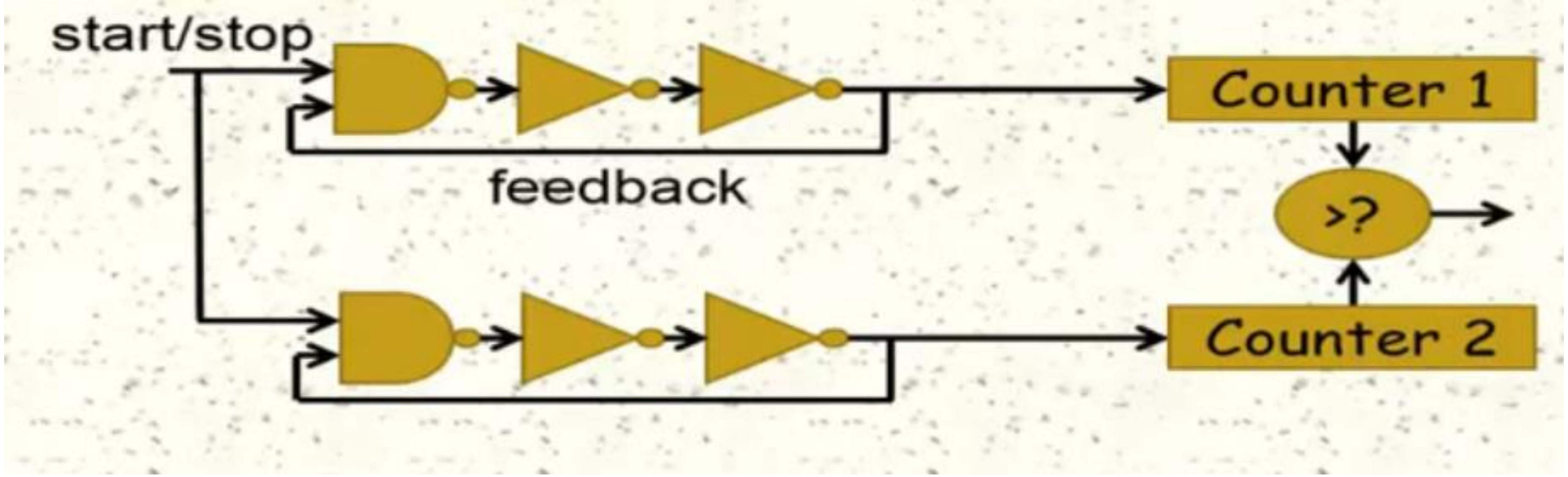


- SRAM PUF
  - SRAM cells naturally settle into a random state on power-up, creating a unique response pattern that can be used as a unique identifier for the device.
- Latch PUF
  - Initially, a=0, b=c=1
  - Changes a to 1
    - If gate 1 is faster, b = 0, c = 1
    - If gate 2 is faster, b = 1, c = 0



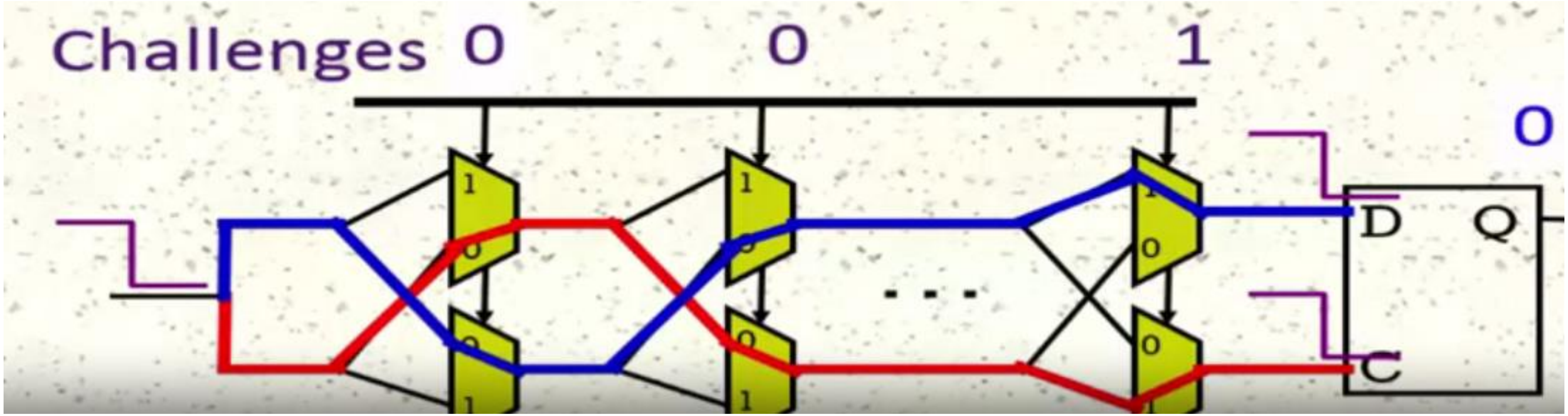
Delay-based PUF

- Ring Oscillator PUF: Use differences in oscillation frequencies of circuits. Ring oscillators oscillate at slightly different frequencies due to manufacturing differences, which form the PUF response.



Arbiter PUF

Use the time difference between two parallel signal paths in a chip to generate unique values. Variations in timing create unique, device-specific responses.



Applications of PUFs

- **Authentication:**
  - PUFs are used for device authentication, ensuring only authorized devices can connect to a network.
  - **Example:** PUF-based authentication in IoT devices, helping prevent unauthorized device access.
- **Key Generation and Storage:**
  - PUFs generate secure cryptographic keys on-demand rather than storing them, reducing the risk of key extraction.
  - **Example:** A PUF in a secure microcontroller generates keys only when needed, enhancing security.
- **Anti-Counterfeiting:**
  - PUFs help verify product authenticity, making it hard to clone or counterfeit physical products.
  - **Example:** PUFs embedded in high-value products (like pharmaceuticals) prevent counterfeiting by verifying product authenticity.

Limitations

- **Environmental Sensitivity:**
  - Changes in temperature, voltage, or physical conditions can sometimes cause inconsistent PUF responses.
  - **Example:** A PUF operating in high temperatures might produce a slightly different response, impacting reliability.
- **Scalability Constraints:**
  - High-quality, stable PUFs are sometimes difficult to scale for mass production without compromising quality or increasing cost.

Thankyou