CS 5432:

Authentication of Inanimate Objects

Fred B. Schneider
Samuel B Eckert Professor of Computer Science

Department of Computer Science
Cornell University
Ithaca, New York 14853
U.S.A.

Authentication of …

- People:
  - Something you **know**, **have**, or **are**.
- Programs running on computers:
  - Something you **know**.
  - Emulation could subvert **have** and/or **are.**
- Computer hardware itself?
    - Authentication needed for establishing a root of trust…

Authentication of Physical Objects

- Paper money
- Nuclear warheads
- Integrated circuit chips

Traditional recipe to prevent counterfeits:

- High **cost** to produce (raw materials)
- Specialized **knowledge** to produce

  … = security by obscurity

New recipe to prevent counterfeits:

- Per-object secret.

Problem Specification

Authenticate a device or document because:

- There is **intrinsic** and **inseparable** identifying information that is unique per object.
  - Information is feasible for verifier to read.
  - Information remains available with use of object.
- Verifier has access to an authenticated copy of this information for making comparisons.

  E.g. serial number "etched" into object and appearing on list.

Application:
Authentication of Paper Money

Today: Bank notes are hard to copy.

- Include watermarks in paper.
- Micro-engraving (printing exceeds resolution of current copying technology)
  - Mask production for VLSI chips undermines this.
- Special paper. US paper includes red and blue silk fibers.

Authentication of Paper Money:
Another Approach: Theory

Abandon: All authentic money is alike.

Embrace: All objects are distinct. Use distinguishing characteristics to identify an authentic object O.

- Measure object O by computing distinct characteristics as prop(O)
- Add label to object O
  - L := k-sign(props(O))
  - Assume props(O+L) = props(O).
- Authenticate O by recomputing prop(O) and checking L.

Overhead: A small number of private keys k must be stored. No need to store inventory of authentics.

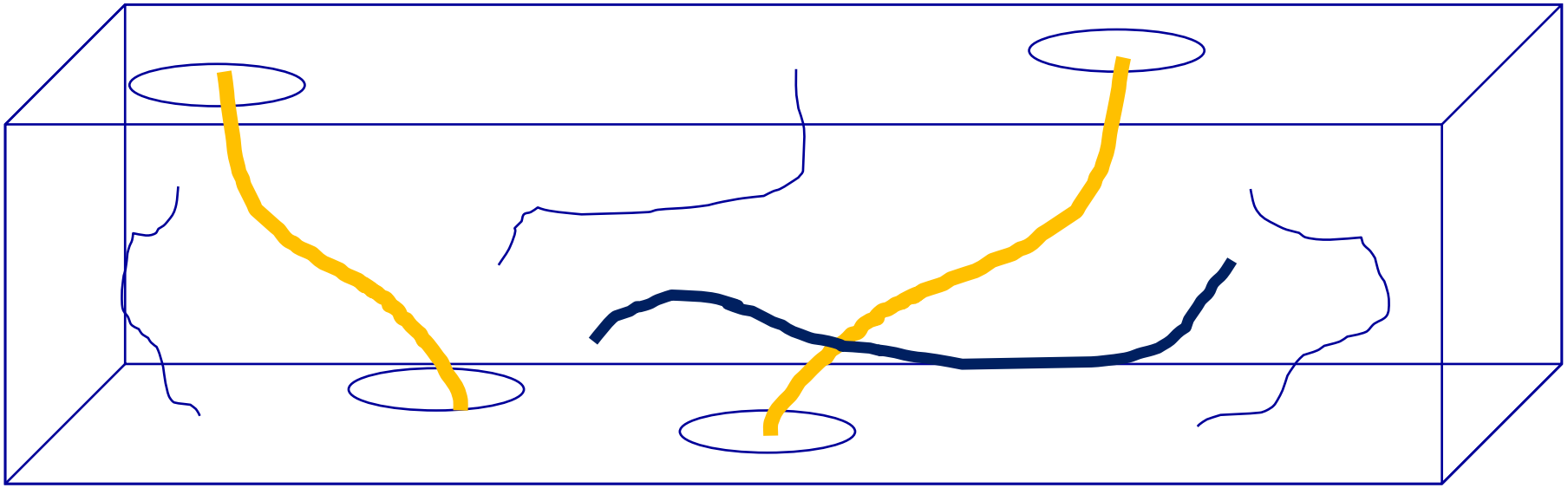
Authentication of Paper Money:

Another Approach: Implementation

Don Bauder [1983] at Sandia Labs…

- Paper is made from pulp.
- Pulp is a slurry of random chopped wood fibers.
- Include random chopped **optical fibers.**
  - Result: Random arrangements of optical fibers.
  - Some fibers transmit light from one side to another.

Bauder's Scheme



- Fingerprint is (x,y) locations of spots on 2 sides.
  - Props(O): set of (x,y) locations on each side
  - Print (invisible ink) k-**sign**(Props(O)) on face of object O
- Authentication requires light + sensor + character reader + public key + computation.

Nuclear Weapons Inventory (RPT)

Developed 1988-91 also by Don Bauder for

INF (Intermediate-range Nuclear Forces Treaty) inspections.

- Treaty signed December 8, 1987.
  - Banned all land-based ballistic missiles, cruise missiles, and missile launchers (but not air- or sea- launched missiles).
- US withdraws August 2, 2019

RPT Scheme

Reflective particle tag (RPT):

- Multifaceted reflective particles in clear paint is applied to a treaty-limited item (TLI)
- When paint dries, particle orientation is fixed.
  - Paint does not cohere, so cannot be peeled off.
- Shining a light on TLI forms a reflective pattern…
  - Tag for each TLI x: props(x) is reflective pattern and tag is produced by k-**sign**(Props(x)) with a private key k.
  - Tags and K are stored by country that must do inventory verification.

Authentication of Chips

Goal: To ensure that a computation occurs on a particular chip (and not using an emulation at some other location).

- The root of trust for any computation is the processor.

Means: Build a tamper-proof alternative to non-volatile memory for storing a secret.

- Storing chip secret would be vulnerable to hw attacks.

PUF Properties

Physical Unclonable Function (PUF): A circuit instance C that translates **fixed**, **unmeasurable**, and **unclonable** properties of a chip instance to a function $F_C(\cdot)$ satisfying:

- Evaluation of $F_C(\cdot)$ always produces the same value.
  - $F_C(\cdot)$ really is a mathematical function!
- Cannot predict $F_C(x)$ from x even with invasive or non-invasive measurements of chip hosting C.
- $F_C(x)$ becomes a different function if chip is modified or probes are attached to the chip.

PUF: Domain of inputs

$F_C(\cdot)$ domain size depends on implementation.

- Size=1: Good for storing a single secret for the chip.
- Size>1: Good for Implementing challenge-response.
  - **weak** PUF: input domain is linear in num of circuit components.
  - **strong** PUF: input domain is exponential in num of circuit components.

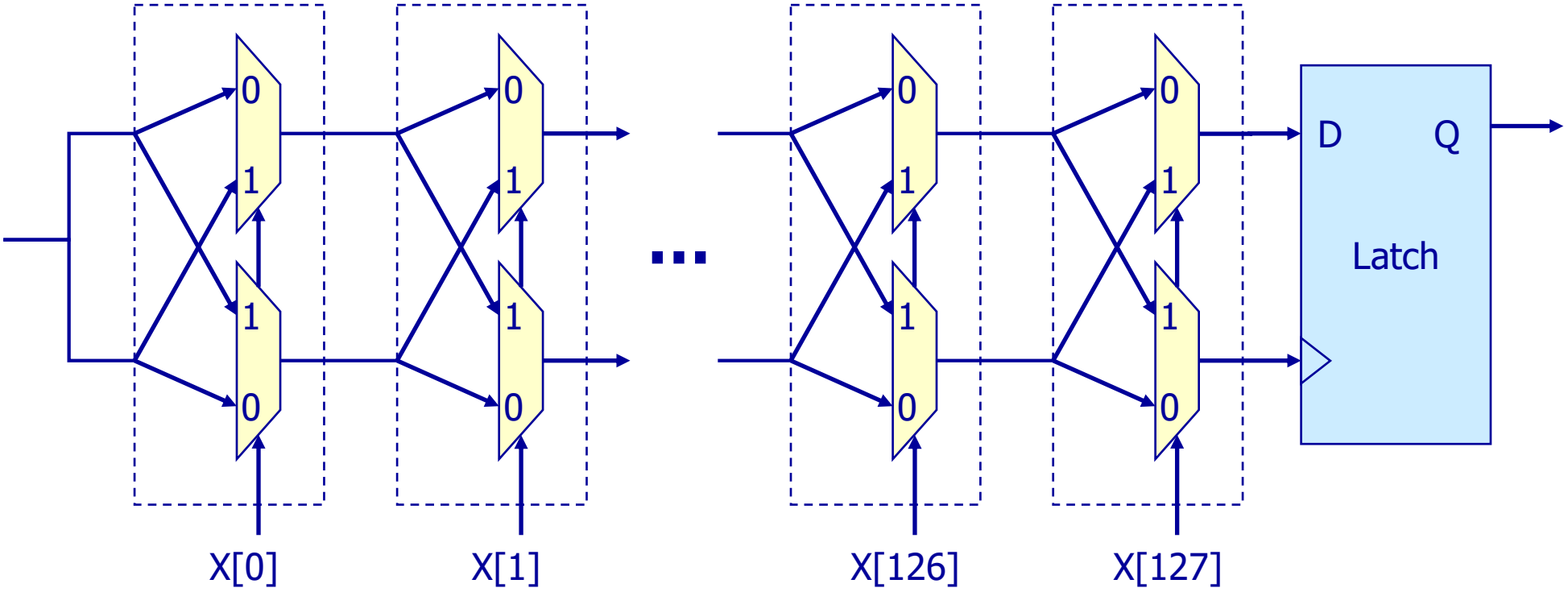
PUF Design: Secret Sauce

Fact: Signal propagation delays in a given silicon IC depend on uncontrollable aspects of chip fabrication.

Suggestion: Build PUF by using circuits that exhibit race conditions!

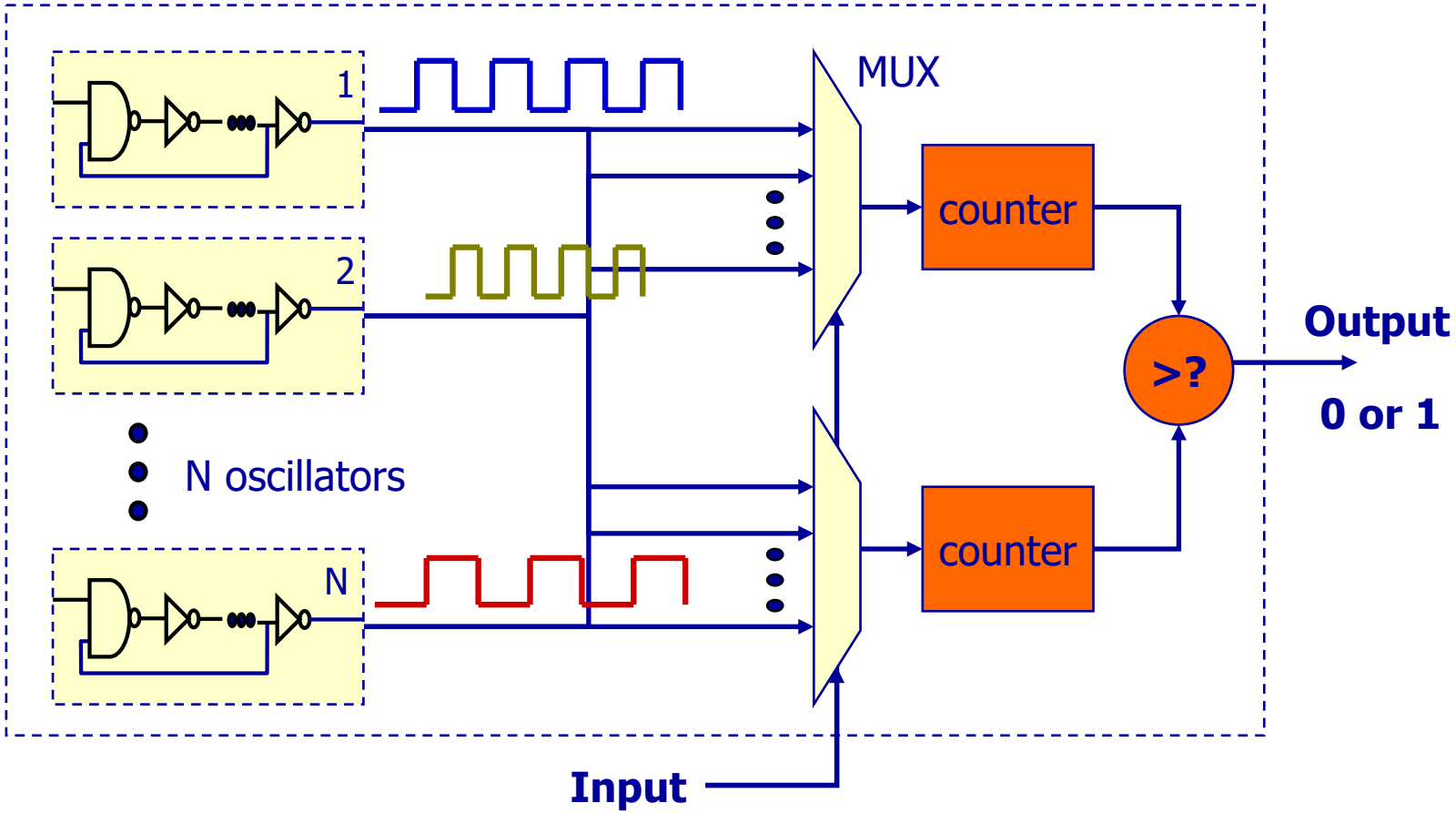
- SRAM PUF (initial value is random)
- Arbiter-based PUF (race condition)
- Ring oscillator PUF (race condition)

Arbiter-based PUF



Arbiter-based PUF

Ring Oscillator PUF



Ring Oscillator PUF

Design Details: Repeatability

Signal delays also affected by environment:

- Operating temperature
- Power supply voltage
- Electrical noise

Mitigations for environmental variation:

- use delay differences rather than absolutes
- use error correcting codes (=redundancy)
- have receiver accept "nearby" values.

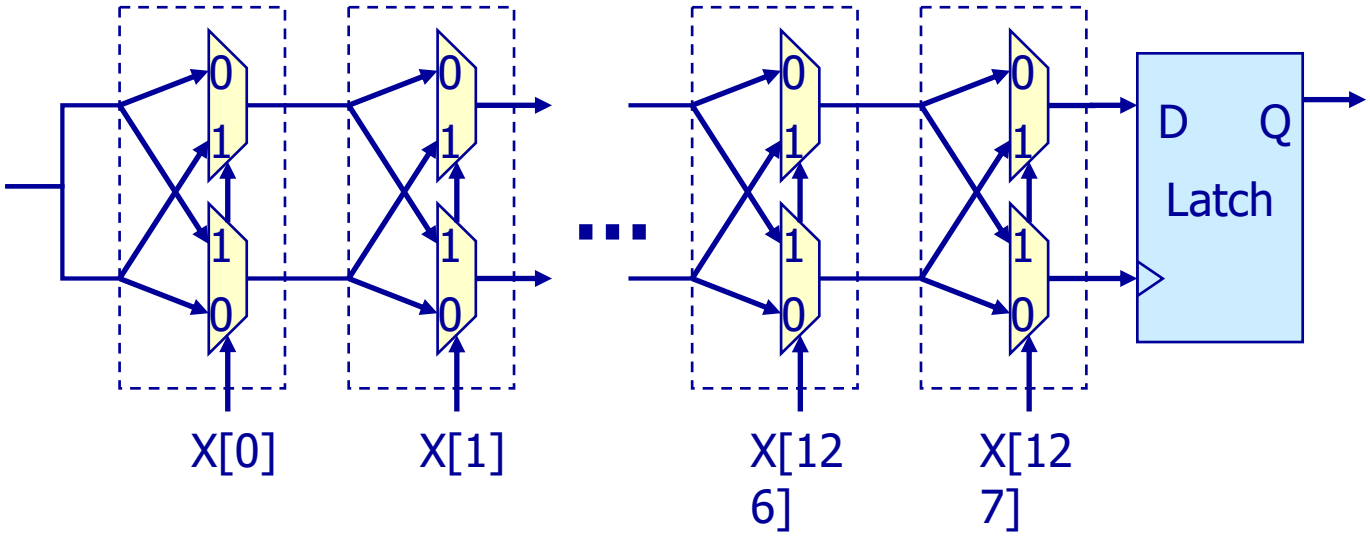
Design Details: Unpredictability

For a function $F_C(\cdot)$ to be deemed **unpredicatable**:

- An attacker who learns some input-output pairs cannot predict outputs for other inputs.
- An attacker must not be able to construct an input that will produce a previously unseen output.

Arbiter-based PUF: Unpredictability

- 2 inputs that differ only in bit i reveal relative speed of stage i → i+1.
- 2n inputs reveal relative speeds of all stages.



Arbiter-based PUF: Unpredictability

- 2 inputs that differ only in bit i reveal relative speed of stage i → i+1.
- 2n inputs reveal relative speeds of all stages.
- $F_C(x)$ can now predict $F_C(x')$ if x and x' differ in a small number of bits (and assuming per stage delays are close.

Mitigations:

- Incorporate a hash function into output path.
- Restrict domain of inputs to eliminate adjacent and problematic inputs. Input domain will become linear.

PUF Applications

PUF can generate an unpredictable bit string of arbitrary length. To amplify length:

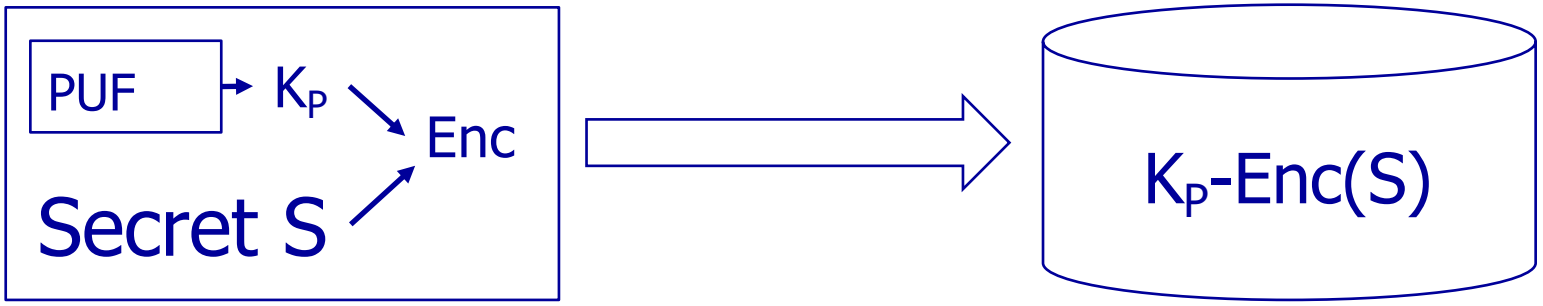
- multiple PUFs
- multiple PUF invocations

Uses for such a bit string:

- Chip identifier
- Chip-specific symmetric key
- Basis for chip-specific public/private key
- Chip-specific seed for random number generator (RNG)

PUF Applications:
Off-Chip Secret Storage

- Chip P uses PUF to generate key K_P.
- K_P materialized in volatile memory only when in use.
  - K_P used to encrypt content before sent off chip.
    - Include timestamp or other nonce to prevent replays.
  - K_P used to decrypt content to reload from off chip.
- Probing chip P causes value of K_P to change.



PUF Applications:
Chip Authentication by Client A

- PUF on chip P uses PUF to generate key K_P.
- K_P is shared with client A
  - Must have a separate key for each client!
- Standard symmetric key authentication protocol:
  1. A → P: K_P-Enc(n) for fresh n
  2. P: m := K_P-Dec(K_P-Enc(n))+1
  3. P → A: K_P-Enc(m)
  4. A: n+1 = K_P-Dec(K_P-Enc(m))
- Probing chip P only will cause value of K_P to change.

PUF Applications:
Chip Authentication w/o Enc 1/2

Enc/Dec circuits require significant chip area…

Avoid K-Enc(·) and K-Dec(·) to authenticate a chip P by using PUF challenge/response…

- Each client A provisioned with a disjoint set CR_A of PUF input/output pairs $(x, F_C(x))$
- Protocol for A to authenticate P.
  - A: remove a pair cr=$(x, F_C(x))$ from CR_A set
  - A → P: x *Challenge x may be used at most once.*
  - P → A: $F_C(x)$ *P generates response by using PUF*
  - A: cr = (x, FC(x)) ?

PUF Applications:

Chip Authentication w/o Enc 2/2

But… need to refresh CR_A periodically.

- **Option 1**: Chip fabricator or system integrator uses chip P to generate a large set of pairs before system deployment.
- **Option 2**: Have chip P support a means to produce sets and export them to customers.

Reading

- Gustavaus J Simmons. Identification of data, devices, documents, and individuals. IEEE Security and Privacy Conference, May 1991, pages 197—218.
- G. Edward Suh and Srinivas Devadas. Physical unclonable functions for device authentication and secret key generation. Proceedings DAC 2007, June 2007. [On course web site]