Security and Cryptography 2022

Mirosław Kutyłowski

V. PHYSICALLY UNCLONABLE FUNCTIONS

Idea: create a device that has a unique unclonable properties.

Applications: authentication, key generation

Early designs- unclonable fingerprints

- **nuclear missiles** - marking them so that copying the fingerprints is impossible, some kind of spray used
- **optical PUFs:** a 1mm material with a large number of randomly positioned 100-m silica

  spheres suspended in a hardened epoxy

  → laser beam directed at a given place with a given polarization

  → reflection depends on spheres encountered by the beam

  → it is practically impossible to reconstruct the same structre of the material

Weak PUFs

– small number of responses

– output of a PUF is a **short** sequence of bits

application -key generation

– secret key is not stored on a device but it is reconstructed on demand

– advantage: no tamper protection needed (lower price), no leakage from the permanent storage

problems

– errors during reconstruction due to physical noise,

– bias of bits

– active attacks (e.g. with a laser beam to change the state of a CMOS circuit implementing PUF)

Strong PUFs

- a big number of CRP (challenge-response pairs)
- outputs for different challenges are almost uncorrelated

application - authentication

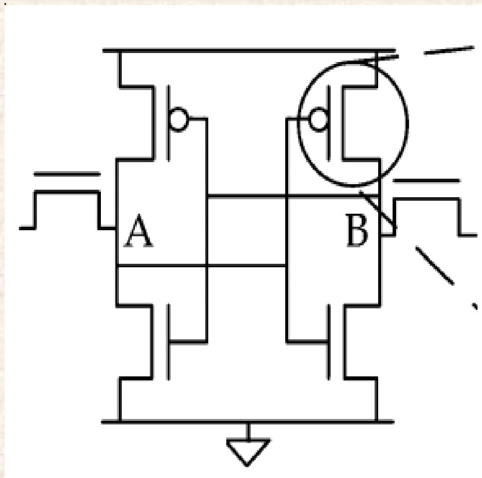
- CRPs read from the device and stored on a server
- each pair used at most once
- advantage: no crypto on the device, lightweight

problems

- errors during reconstruction due to physical noise,
- reconstruction of the model (without creating a physical copy)
- active attacks

SRAM PUF

- at power-up both states (0 and 1) are possible
- which one will prevail depends on a random processes, in practice: bias towards 1
- attacks: keep a given value for 10 hours, after the next power-up bias towards the other bit



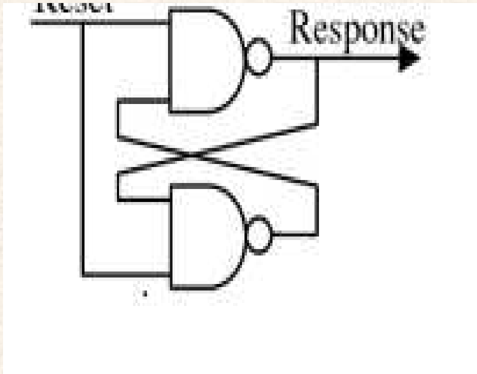
(picture from Heder et al.: Physical unclonable Functions and applications)

advantages and disadvantages:

- low price, low area
- high error rate,
- error correction codes applied, but keeping syndrome codes themselves are leaking inforamtion

Strong PUFs

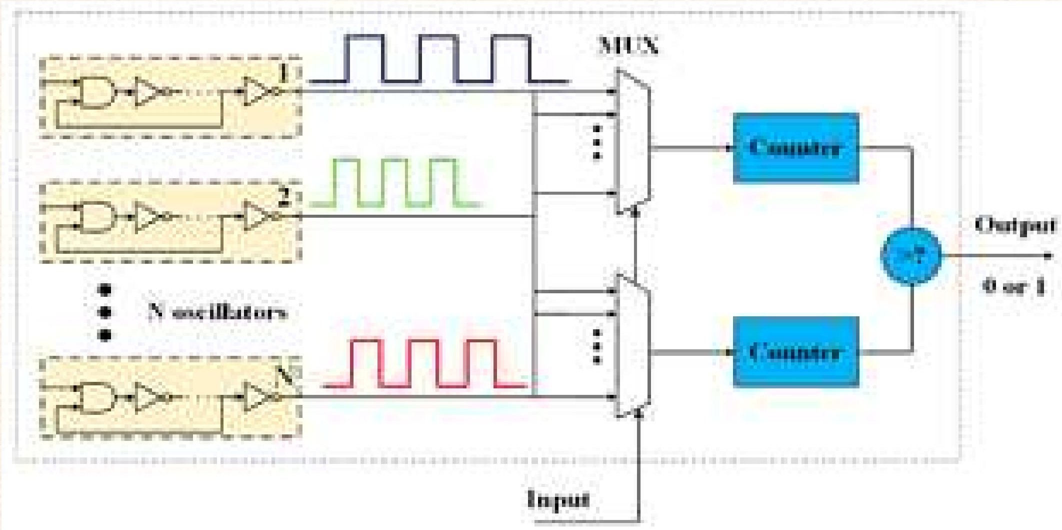
similar solution based on bistable latches composed of 2 NAND gates:



SR Latch:

- notation: reset=a, outputs from gates: b, c
- initially: a=0, b=c=1
- change a to 1, then
  - b=1, c=0 if lower gate faster
  - b=0, c=1, if upper gate faster

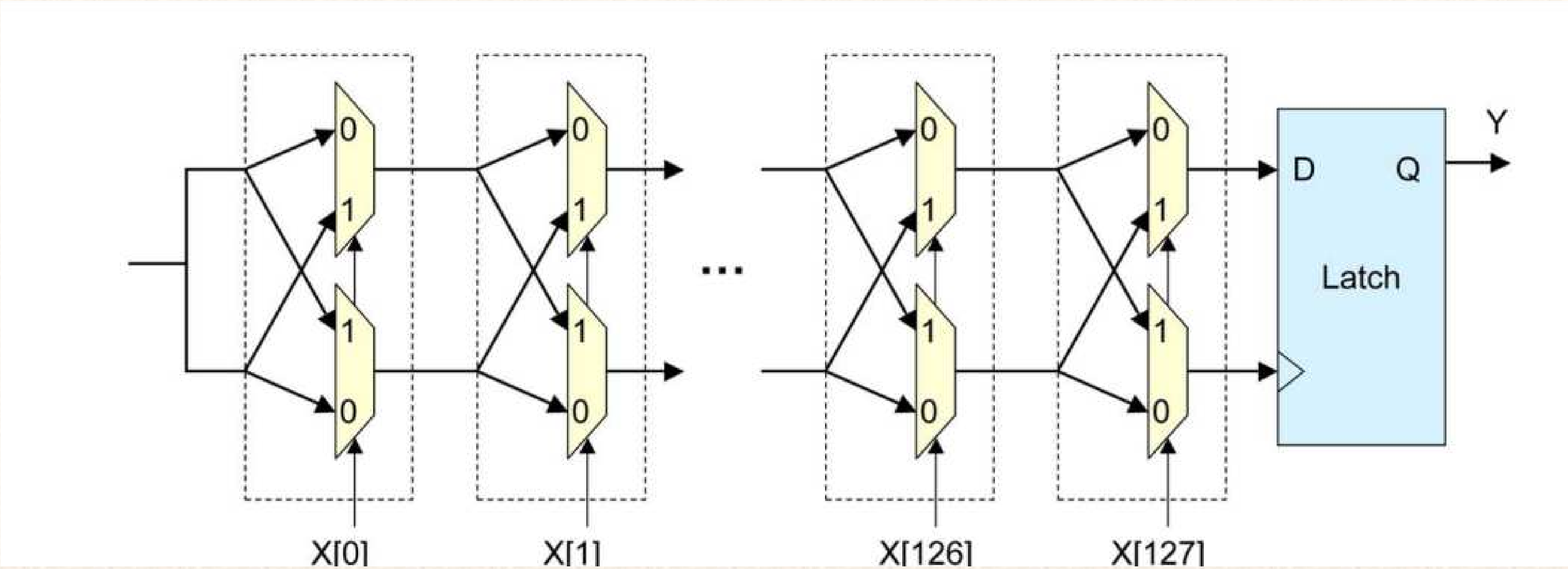
Ring Oscilators



(fig. from cryptostack exchange)

- each oscilator has a different speed
- ordering the speeds is the output secret of the PUF
- problem: if frequences are almost the same then noise becomes important

Arbiter PUF



(picture from Heder et al.: Physical unclonable Functions and applications)

– input X determines the paths

Arbiter PUF

Problems

- delays on each edge determine behavior
- modelling by linear equations,
- each experiment yields 2 equations
- linear algebra problem, easy to solve

Countermeasures

- combine a number of Arbiter PUFs with XOR (cascade of XOR gates)
- other non-linearity

Further Problems

- machine learning attacks – very effective, XOR makes them less effective (time increases exponentially with the number of XOR gates
- ML + side channel information – Arbiter PUF easy to break even if many XOR gates

Model based PUF

- instead of holding CRP in a (protected) database ⟨text-dots⟩
- ⟨text-dots⟩ make the model for a PUF public (e.g. delays for Arbiter PUF)

idea for authentication

1. the server creates a challenge x
2. the PUF rapidly computes $f(x)$ thanks to hardware
3. the server receives the answer and recomputes $f(x)$ (tedious and long computation)

Problem:

find a PUF that:

- is fast on hardware
- cannot be cloned
- software computation is unproportionally long on any reasonable machine*

*reasonable = regarding the price with respect to the profit

Patent problems

killing the idea through legal threats

available on some hardware platforms