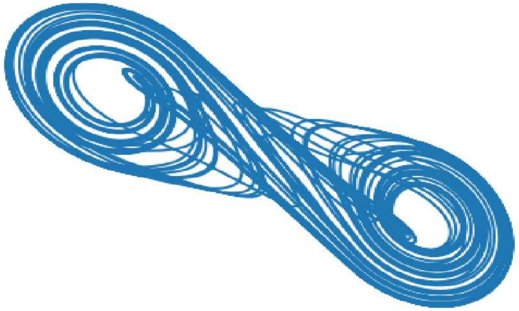
SAND2018-13455PE

Physical Unclonable Functions for Cryptographic Key Generation

Physics and Information Theoretic Considerations



Calvin Chan
Rachel Dondero
Jason Hamlet
Ryan Helinski
Mark Torgerson
Will Zortman

Advanced Science & Technology
Nuclear Deterrence
Global Security
National Security Programs
Energy & Homeland Security

Sandia National Laboratories

Exceptional service in the national interest

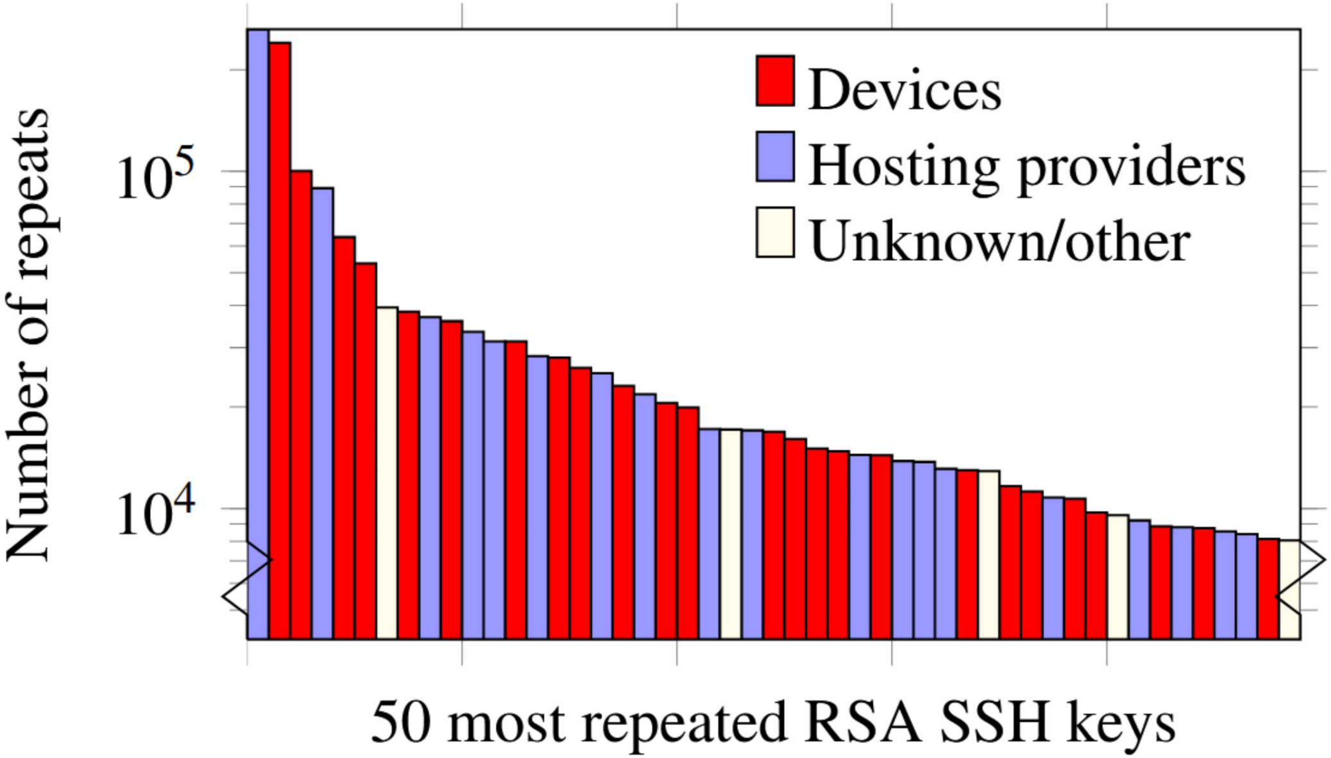
U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Keys: The Entropy Problem

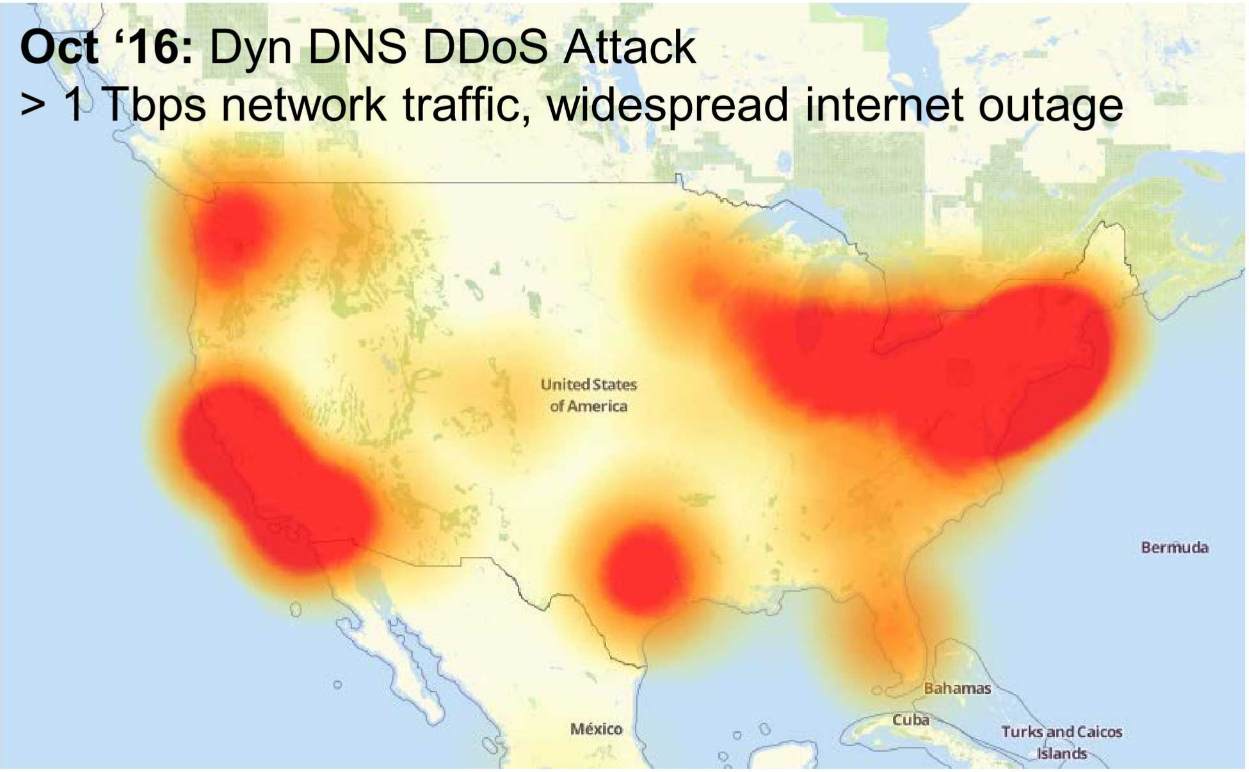
- Linux Random Number Generator (RNG): Failure in Entropy
  - Servers, IoT devices
  - Insufficient diversity of devices and environments → insufficient entropy
  - Weak/common TLS/SSH keys, usually generated on first boot



N Heninger, et al., “Mining Your Ps and Qs”, USENIX (2012)

Keys: The Uniqueness Problem

- Mirai Botnet: Failure in Identity and Key Management
  - Internet-of-Things (IoT) devices, i.e., routers, webcams
  - 60+ common default usernames (identities) and passwords (keys)
  - 600,000 devices hijacked for Distributed Denial of Service (DDoS) attacks



Oct '16: Dyn DNS DDoS Attack
> 1 Tbps network traffic, widespread internet outage

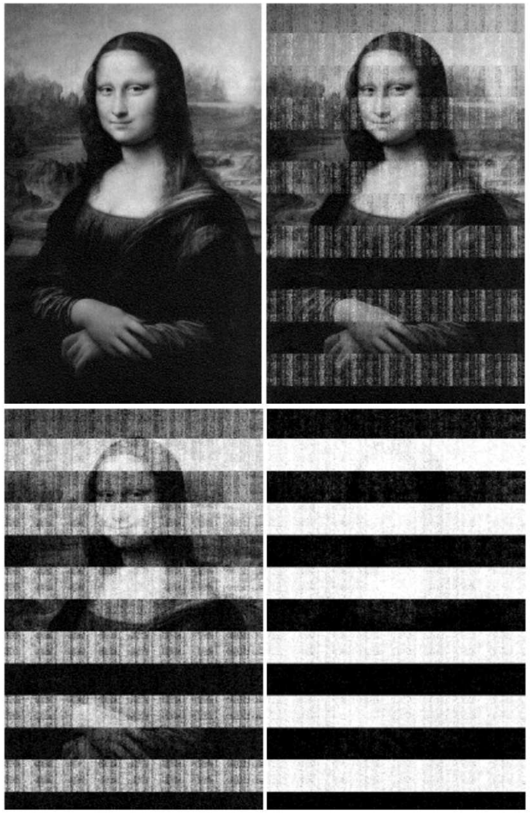
```
admin
administrator
root
user
<null>
…
```

```
password
    1234
   12345
   admin
  <null>
       …
```

L3 Communications Outage Map

Keys: The Storage Problem

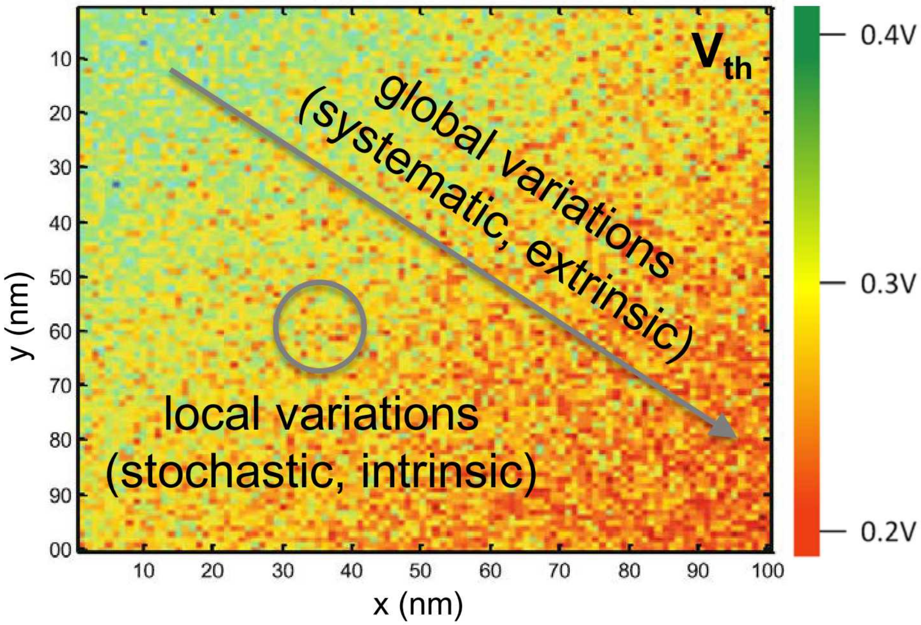
- Cold Boot Attack: Failure in Secure Key Storage
  - Dynamic Random Access Memory (DRAM)
  - Data retention extended from seconds to minutes by lowering temperature
  - Recovered AES, DES, and RSA keys stored in memory



A. Halderman, et al., “Cold Boot Attacks on Encryption Keys”, USENIX (2009)

Physical Unconable Functions (PUFs)

- Semiconductor, a.k.a. Integrated Circuit PUFs
  Proposed solution to key entropy / identity / storage problems
  - **Entropy:** Manufacturing variations in semiconductor materials, e.g., doping, oxide thickness, roughness
  - **Identity:** Capture these variations using semiconductor devices to form a digital fingerprint

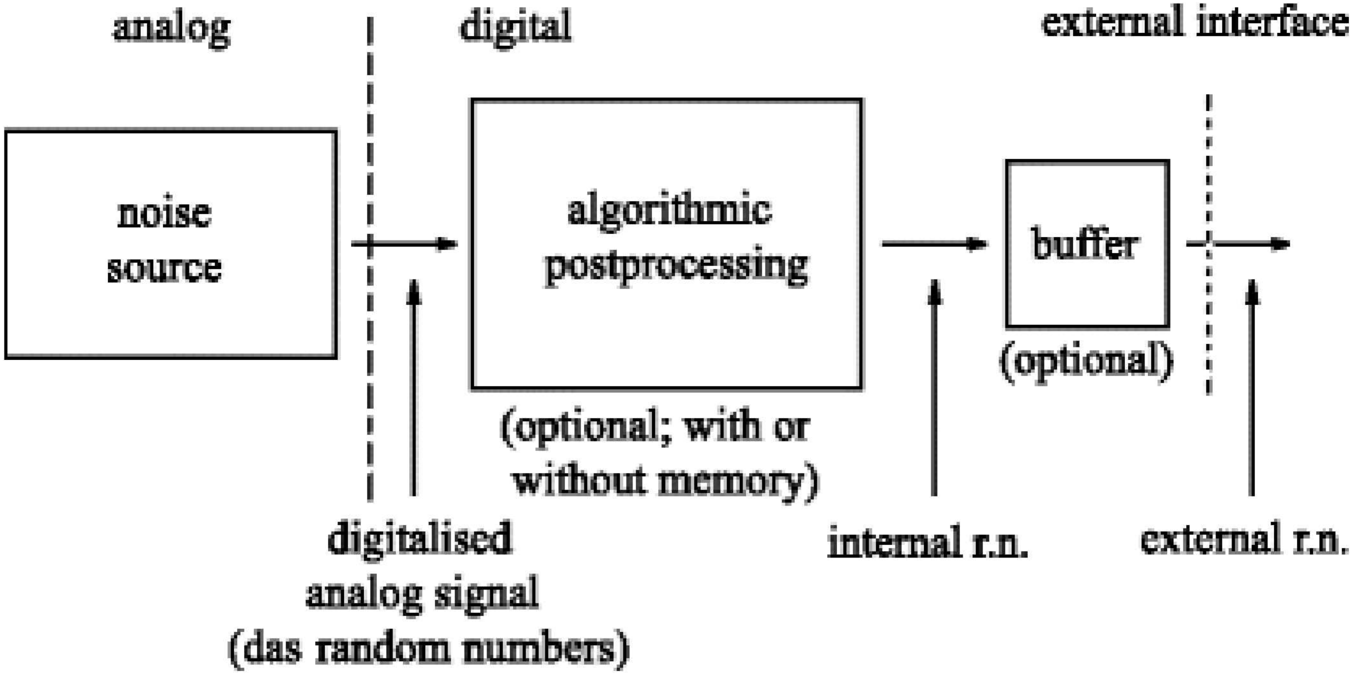


- **Storage:** Keying material stored as intrinsic materials properties
  Keys dynamically generated on the fly, never stored in memory

Bohm & Hofer, *Physical Unclonable Functions in Theory and Practice*, DOI: 10.1007/978-1-4614-5039-9, Springer (2013).

Key Generation with PUFs

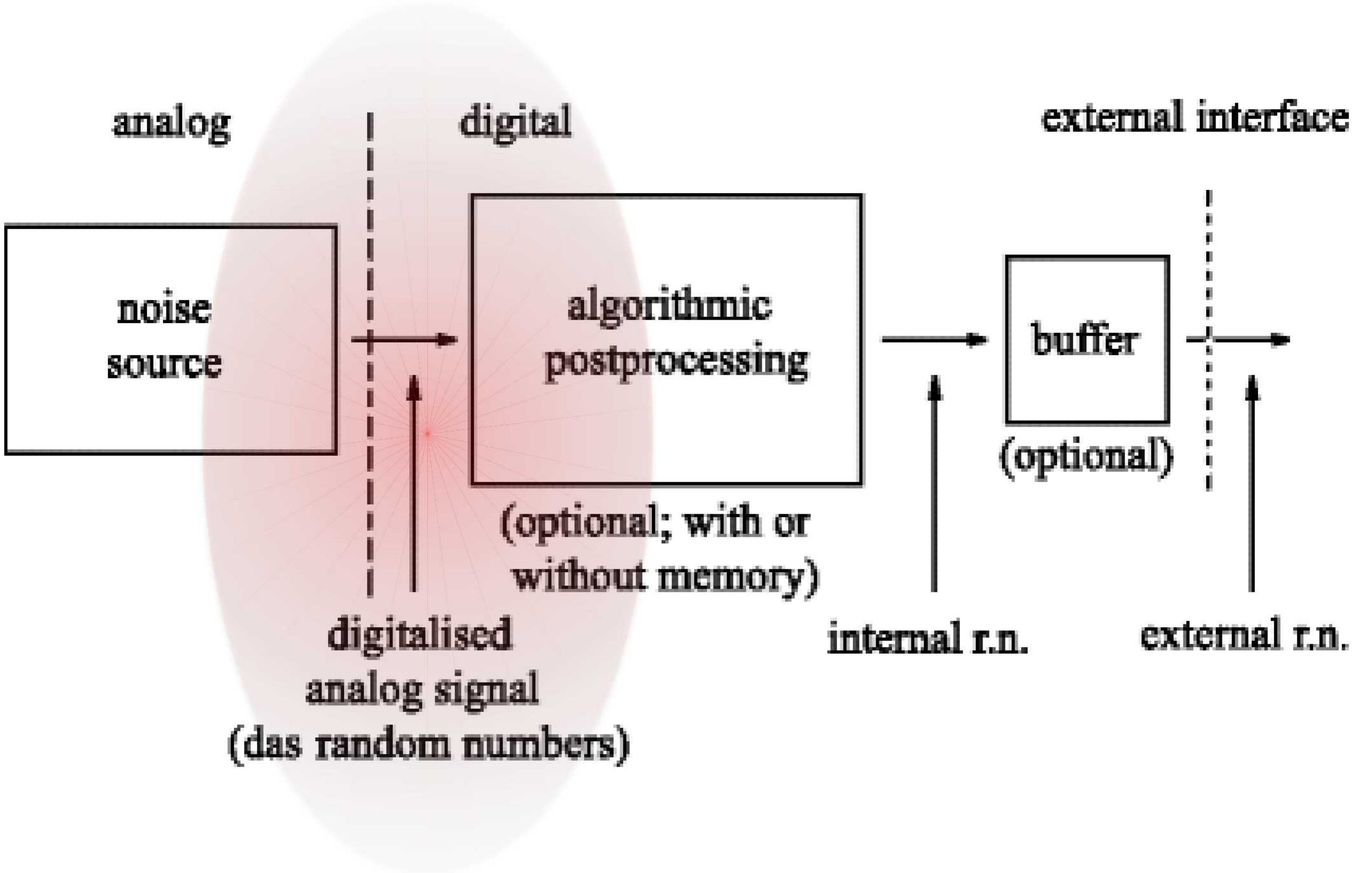
- Keys should be *n*-bits long depending on security requirements
- Keys should be independently, identically distributed (IID)
- Keys should remain the same throughout the duration of use


analog
digital
external interface
noise source
algorithmic postprocessing
buffer
(optional)
(optional; with or without memory)
digitalised analog signal (das random numbers)
internal r.n.
external r.n.

Koc (ed.), *Cryptographic Engineering*, DOI: 10.1007/978-0-387-71817-0, Springer-Verlag (2009).

Key Generation with PUFs

- Keys should be *n*-bits long depending on security requirements
- Keys should be independently, identically distributed (IID)
- Keys should remain the same throughout the duration of use

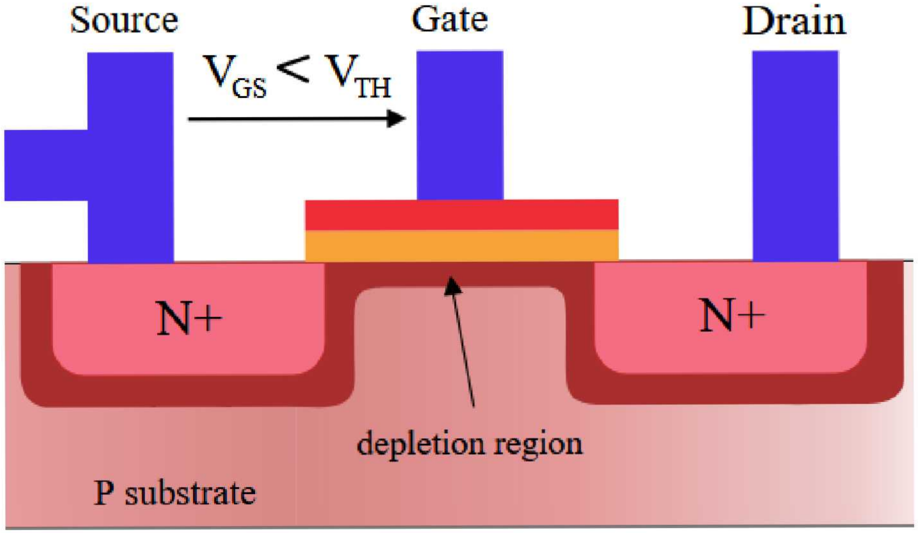

analog
digital
external interface
noise source
algorithmic postprocessing
buffer
(optional)
(optional; with or without memory)
digitalised analog signal (das random numbers)
internal r.n.
external r.n.

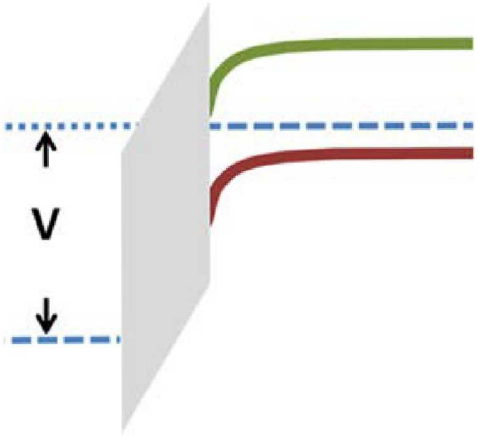
Koc (ed.), *Cryptographic Engineering*, DOI: 10.1007/978-0-387-71817-0, Springer-Verlag (2009).

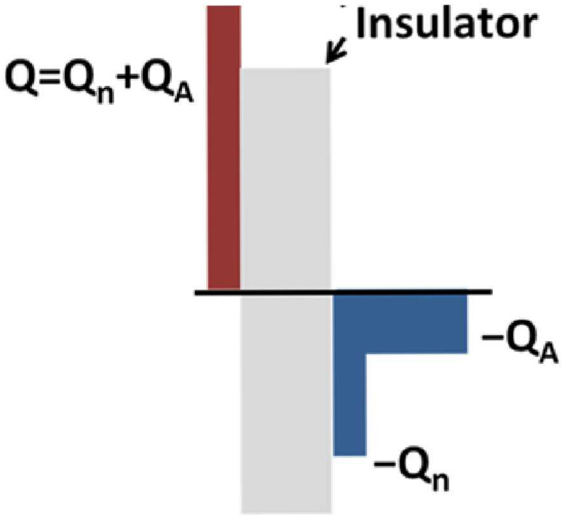
Integrated Circuit PUFs

- Metal-Oxide-Semiconductor (MOS) Transistor is the fundamental readout device in IC PUFs

nFET





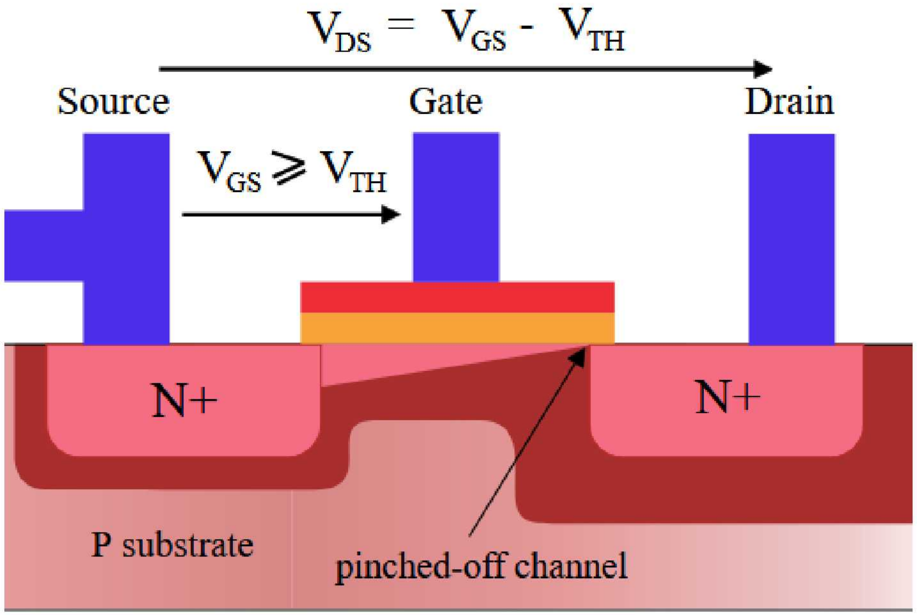


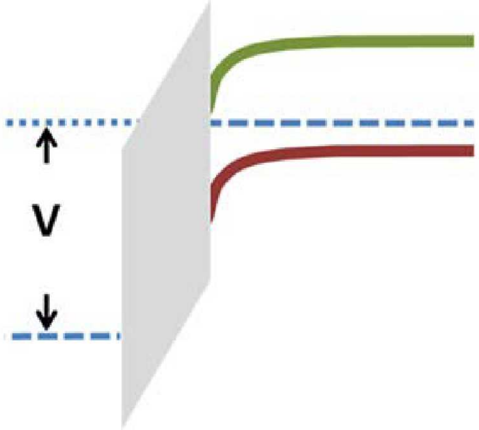
$$I_D = \frac{\mu_n C_{ox}}{2}\frac{W}{L}[V_{GS} - V_{th}]^2\,[1 + \lambda(V_{DS} - V_{DSsat})]$$

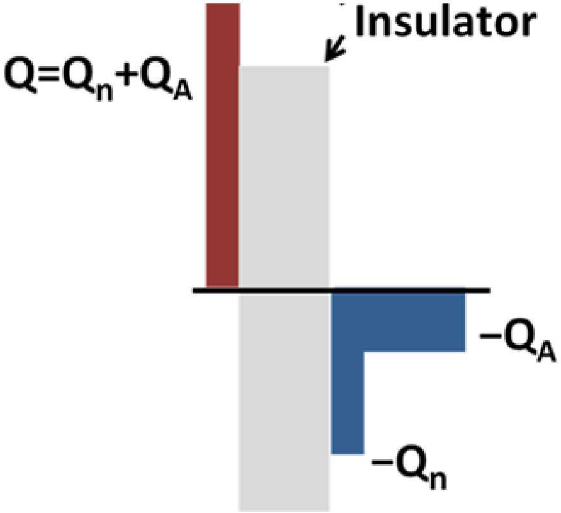
Integrated Circuit PUFs

- Metal-Oxide-Semiconductor (MOS) Transistor is the fundamental readout device in IC PUFs

nFET



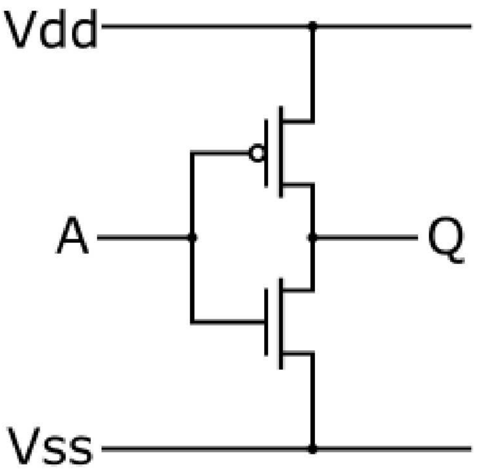


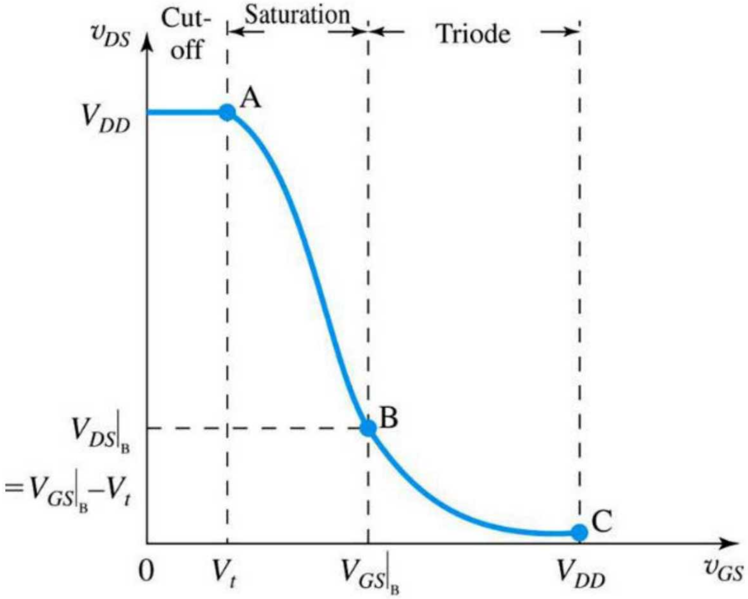


$$I_D = \frac{\mu_n C_{ox}}{2}\frac{W}{L}[V_{GS} - V_{th}]^2\,[1 + \lambda(V_{DS} - V_{DSsat})]$$

Integrated Circuit PUFs

- Metal-Oxide-Semiconductor (MOS) Transistor is the fundamental readout device in IC PUFs





Weak Inversion

$$I_D \approx I_{D0} e^{\frac{\kappa(V_G - V_{th}) - V_S}{V_T}}, \quad \kappa = \frac{C_{ox}}{C_{ox} + C_D}$$

Linear/ Triode

$$I_D = \mu_n C_{ox} \frac{W}{L}\left((V_{GS} - V_{th})\, V_{DS} - \frac{{V_{DS}}^2}{2} \right)$$

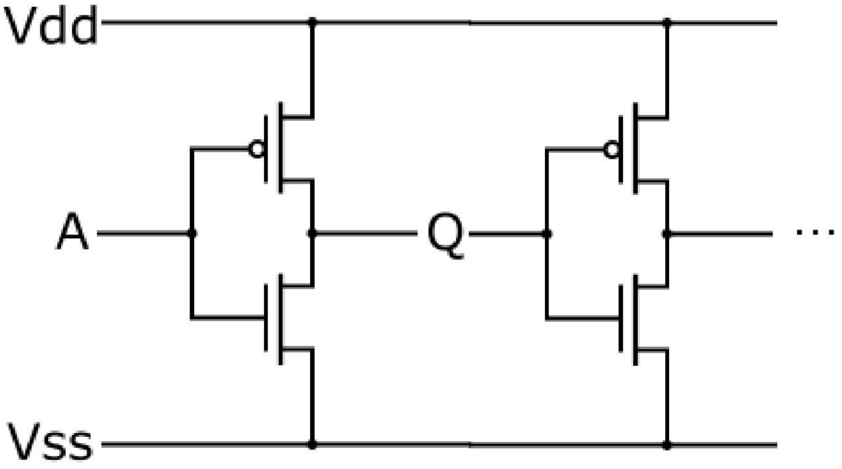
Saturation

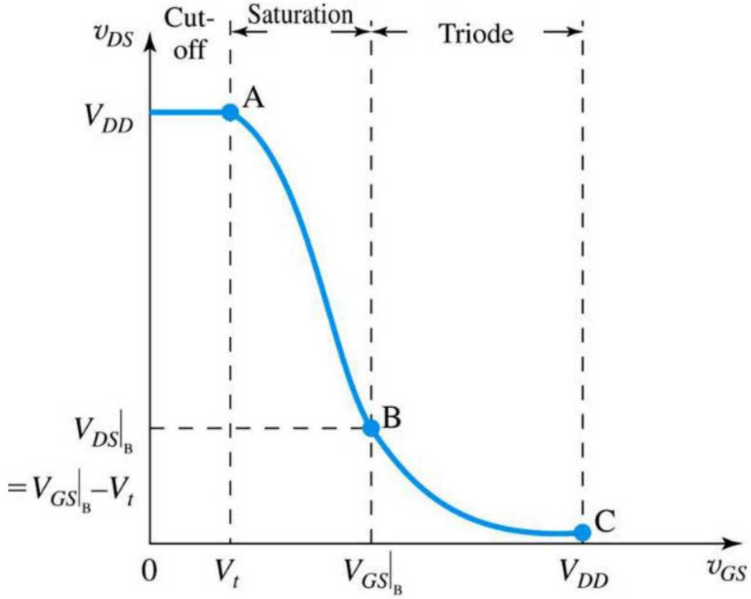
$$I_D = \frac{\mu_n C_{ox}}{2} \frac{W}{L} [V_{GS} - V_{th}]^2 \, [1 + \lambda(V_{DS} - V_{DSsat})]$$

Sedra & Smith, *Microelectronic Circuits*, 6th Ed., Oxford (2009).

Integrated Circuit PUFs

- Metal-Oxide-Semiconductor (MOS) Transistor is the fundamental readout device in IC PUFs





Weak Inversion

$$I_D \approx I_{D0} e^{\frac{\kappa(V_G - V_{th}) - V_S}{V_T}}, \quad \kappa = \frac{C_{ox}}{C_{ox} + C_D}$$

Linear/ Triode

$$I_D = \mu_n C_{ox} \frac{W}{L} \left((V_{GS} - V_{th}) V_{DS} - \frac{V_{DS}{}^2}{2} \right)$$

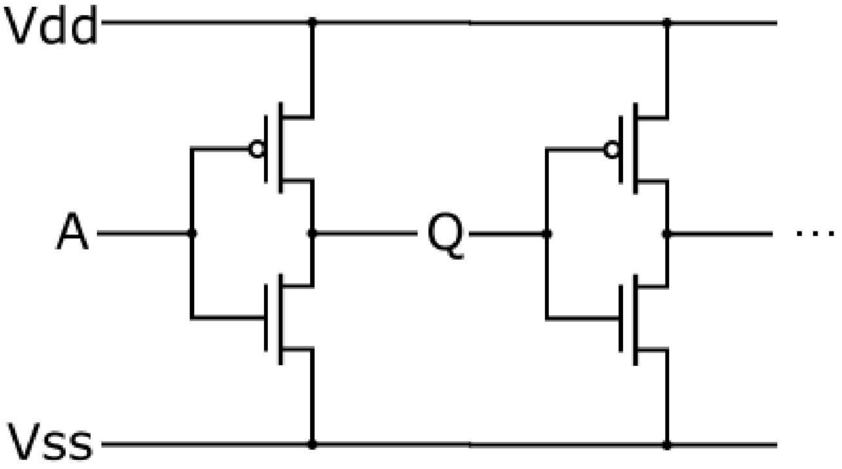
Saturation

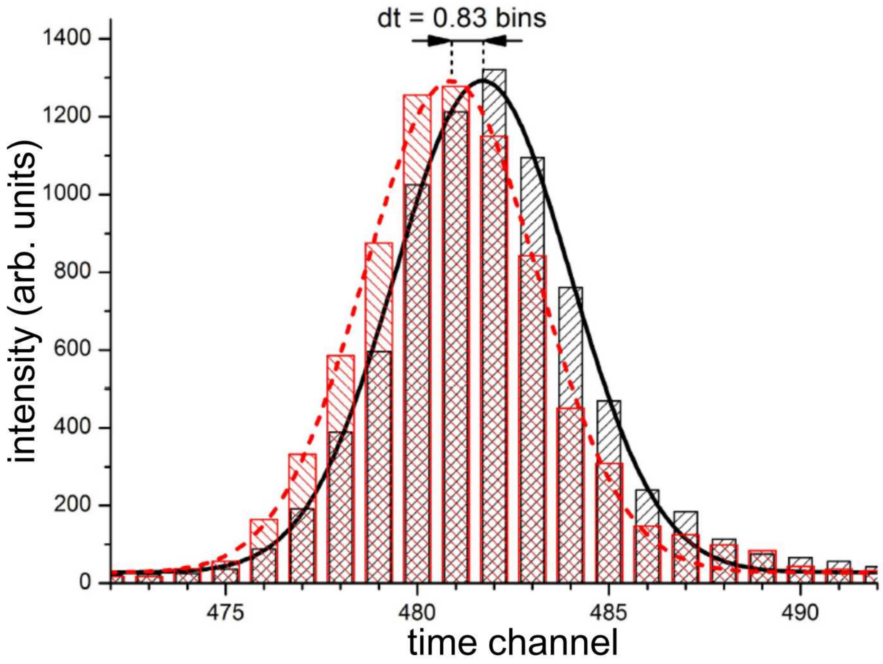
$$I_D = \frac{\mu_n C_{ox}}{2} \frac{W}{L} [V_{GS} - V_{th}]^2 [1 + \lambda(V_{DS} - V_{DSsat})]$$

Sedra & Smith, *Microelectronic Circuits*, 6th Ed., Oxford (2009).

Integrated Circuit PUFs

- Metal-Oxide-Semiconductor (MOS) Transistor is the fundamental readout device in IC PUFs





Complex non-linear relationships define propagation delay

~ 1's to 10's picosecond

Very difficult to predict *a priori* (theory/modeling)
Very difficult to measure *a posteriori* (empirically)

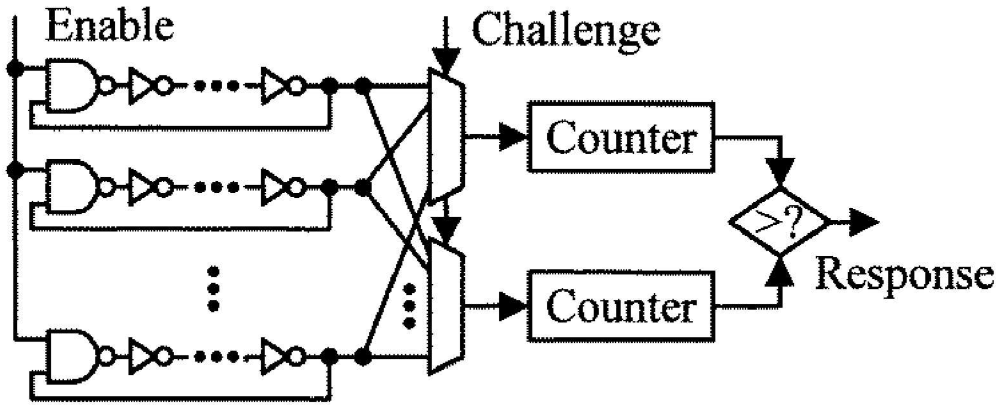
Tajik et al., *CHES*, LNCS 8731, pp. 493–509, (2014).

Delay Based PUF

- **Ring Oscillator PUF**

  Based on RO TRNG
  Compares frequency of 2 ROs
  Challenge-Response Pairs (CRPs):

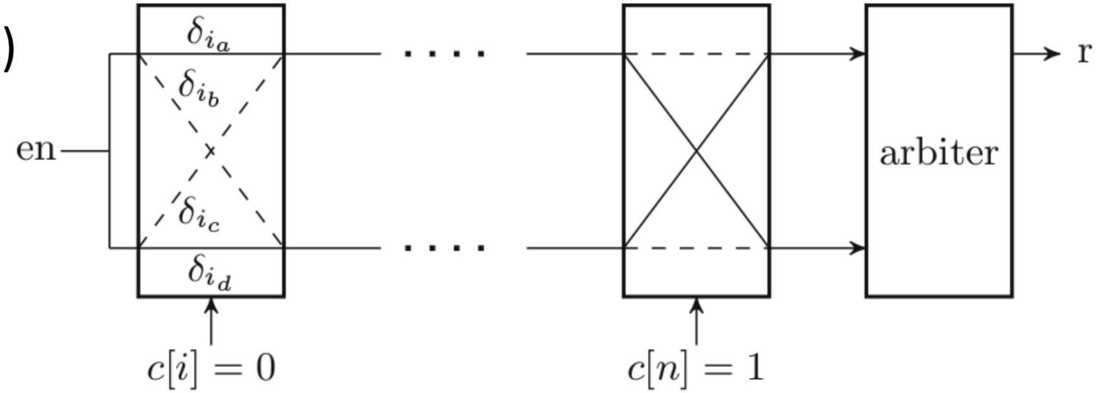
$$\binom{n}{2}$$



- **Arbiter PUF**

  Element pairwise paths (MUX)
  Race between two nominally identical paths
  Challenge-Response Pairs (CRPs):

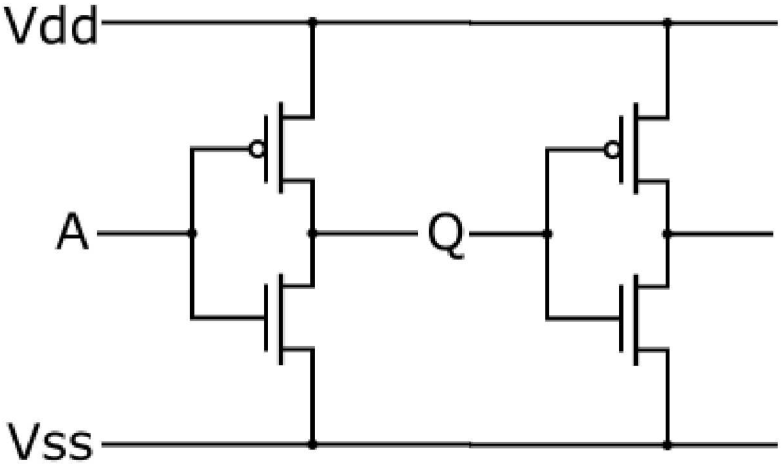
$$2^n$$



Bauer & Hamlet, “Physical Unclonable Functions: A Primer,” *IEEE Security & Privacy*, Nov/Dec 2014.

State Based PUF

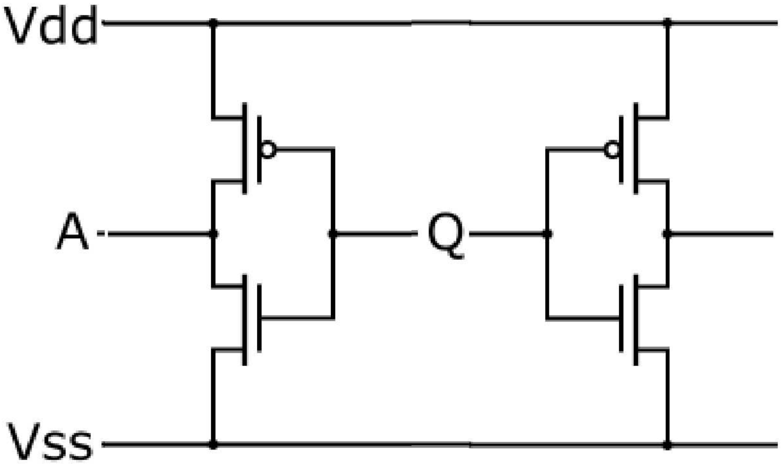
- **Static Random Access Memory (SRAM) PUF**



Cross-coupled inverters
Imbalanced transient determines
power-on state of cells
Challenge-Response Pairs
(CRP): **1**

State Based PUF

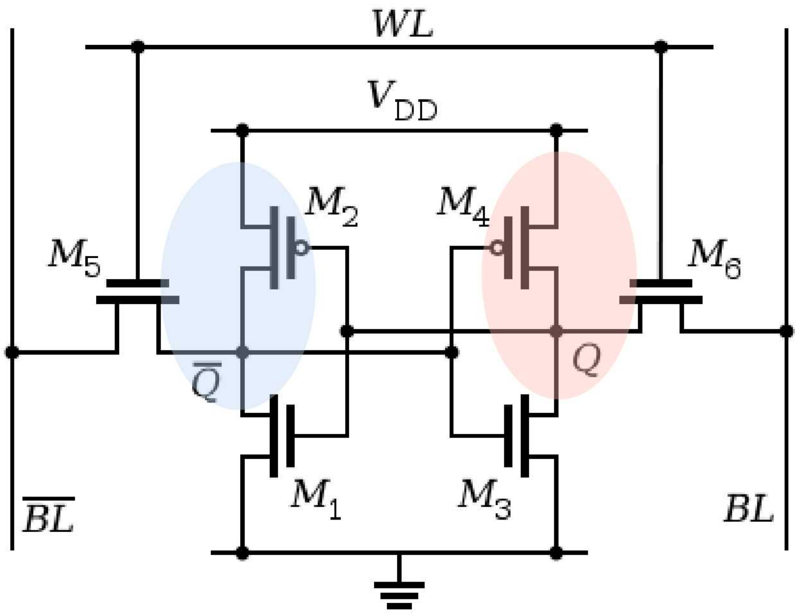
- **Static Random Access Memory (SRAM) PUF**

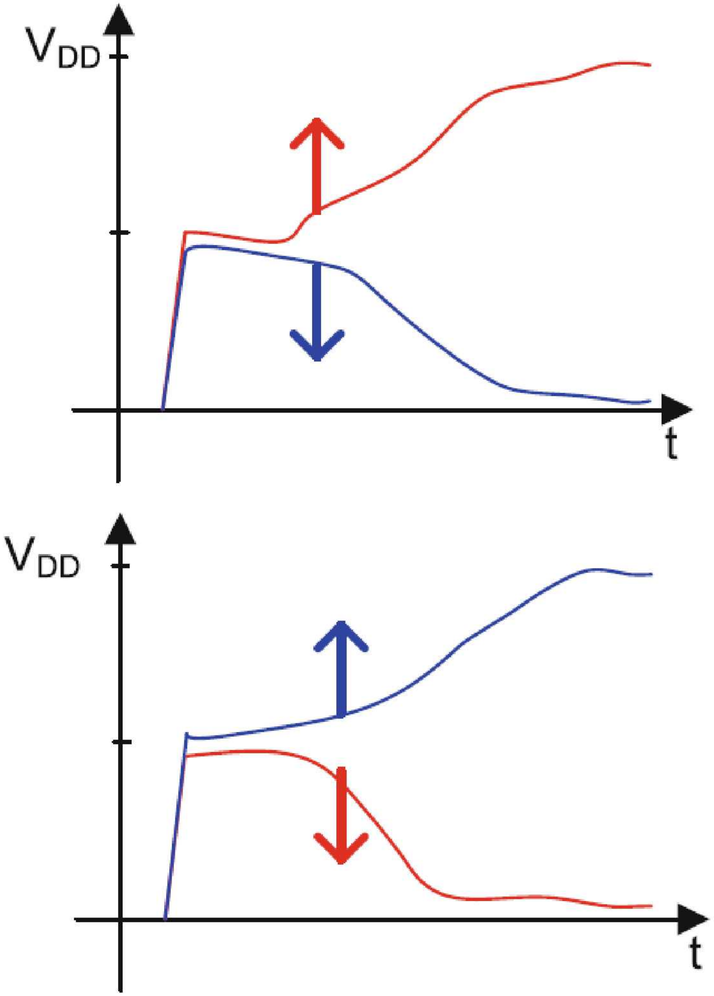


Cross-coupled inverters
Imbalanced transient determines power-on state of cells
Challenge-Response Pairs (CRP): **1**

State Based PUF

- **Static Random Access Memory (SRAM) PUF**





Cross-coupled inverters

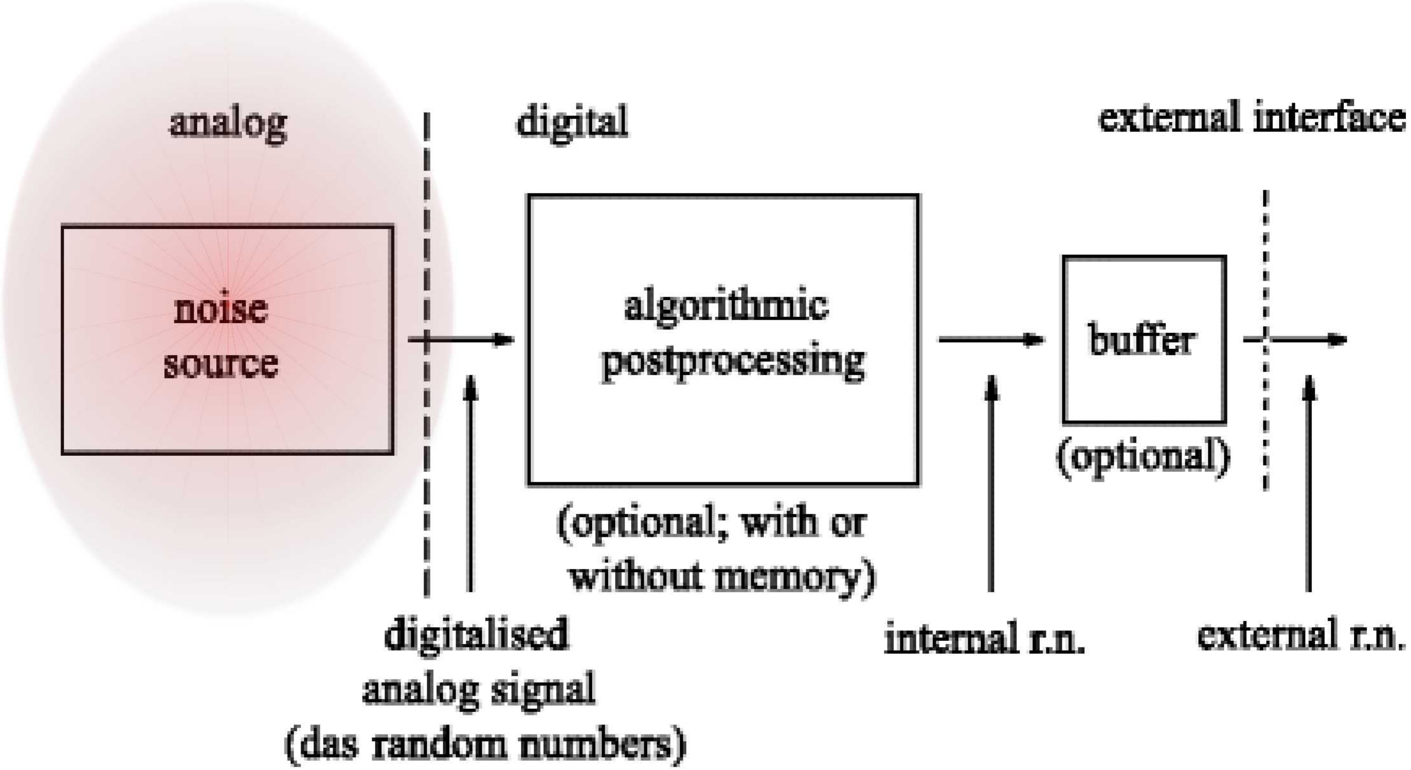
Imbalanced transient determines power-on state of cells

Challenge-Response Pairs (CRP): **1**

Bohm & Hofer, *Physical Unclonable Functions in Theory and Practice*, DOI: 10.1007/978-1-4614-5039-9, Springer (2013).

Key Generation with PUFs

- Keys should be *n*-bits long depending on security requirements
- Keys should be independently, identically distributed (IID)
- Keys should remain the same throughout the duration of use

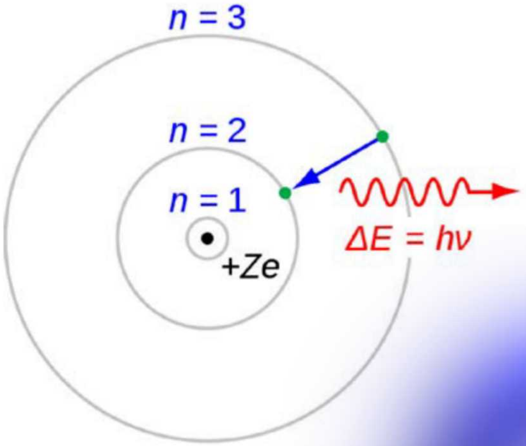

analog
digital
external interface
noise source
algorithmic postprocessing
buffer
(optional)
(optional; with or without memory)
digitalised analog signal (das random numbers)
internal r.n.
external r.n.

Koc (ed.), *Cryptographic Engineering*, DOI: 10.1007/978-0-387-71817-0, Springer-Verlag (2009).

Noise Sources

- Two **fundamental** sources of noise
  - **Quantum mechanics**
    Shot noise

    Single photon detection
    Electrons tunneling
    Nuclear decay



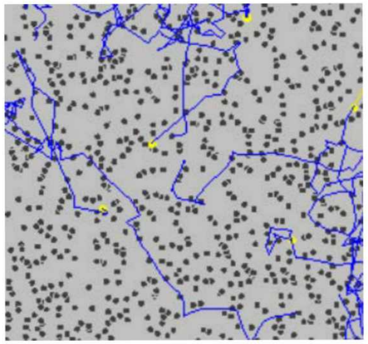
$$\psi_{nlm}(r,\vartheta,\varphi) = \sqrt{\left(\frac{2}{na_0}\right)^3 \frac{(n-l-1)!}{2n[(n+l)!]}}\, e^{-\rho/2}\rho^l L^{2l+1}_{n-l-1}(\rho)\cdot Y_{lm}(\vartheta,\varphi)$$

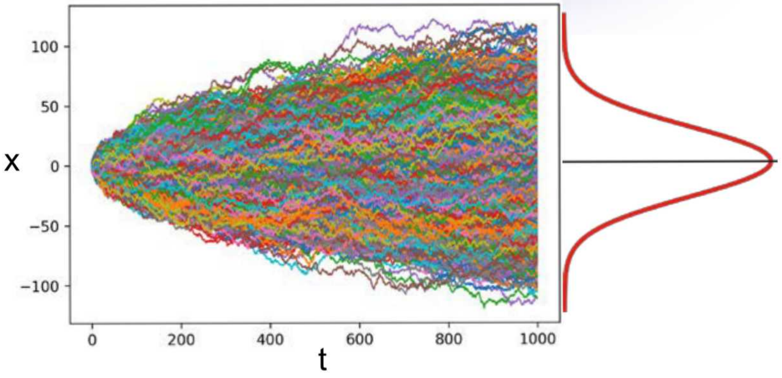
  - **Thermal mechanics**
    Johnson-Nyquist noise

    Thermionic emission
    Avalanche noise
    Atmospheric noise

$$\rho(x,t) = \frac{N}{\sqrt{4\pi Dt}} e^{-\frac{x^2}{4Dt}}$$

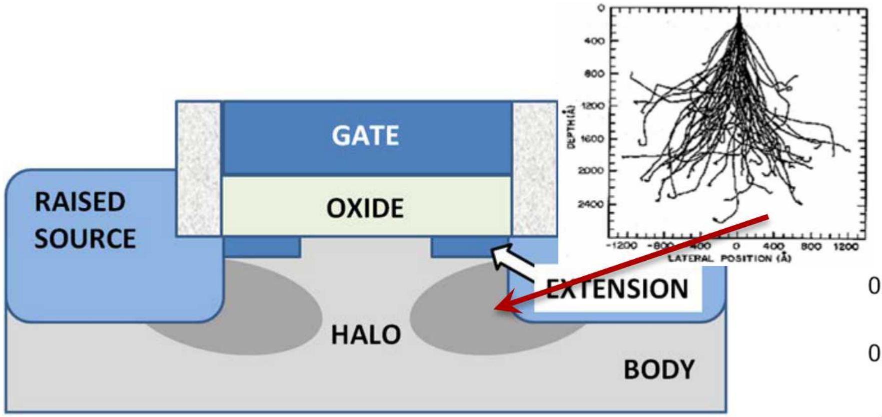
$$D = \mu k_B T$$



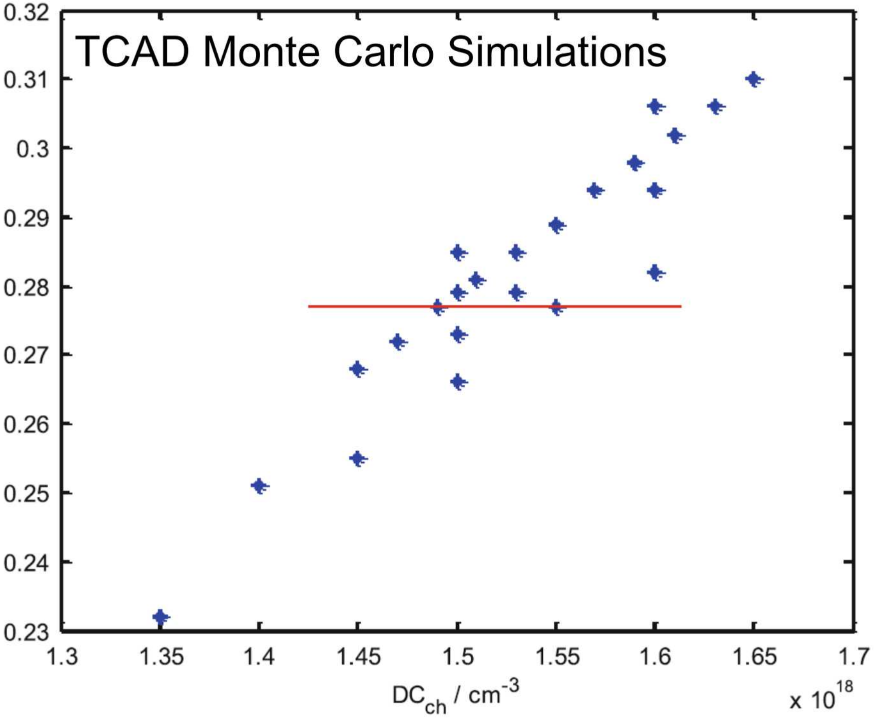


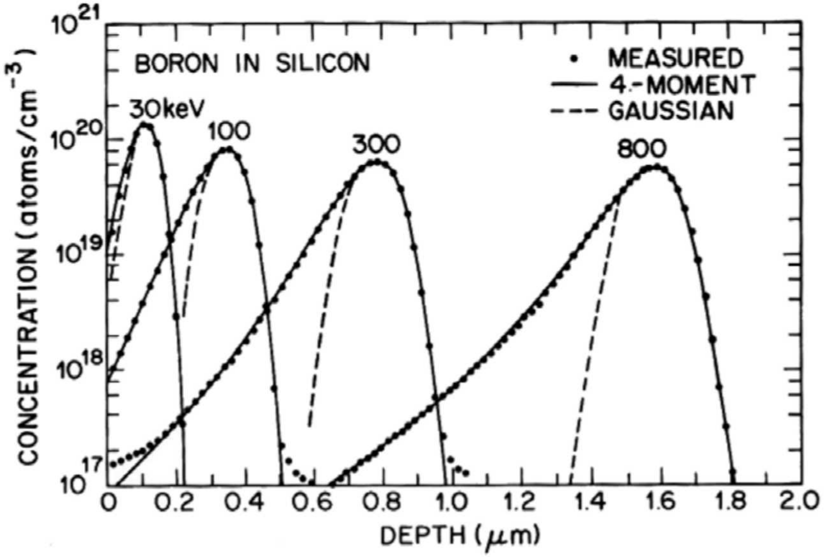
Noise Sources

- "Manufacturing variations" **ARE NOT** fundamental noise sources
  Manufacturing processes **may** contain fundamental noise sources



$$V_{th} \propto \frac{\sqrt{2\epsilon_s q N_a (2\varphi_B + V_{ox})}}{C_{ox}}$$



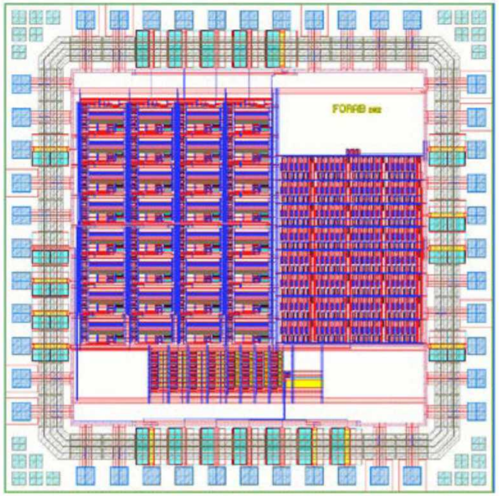


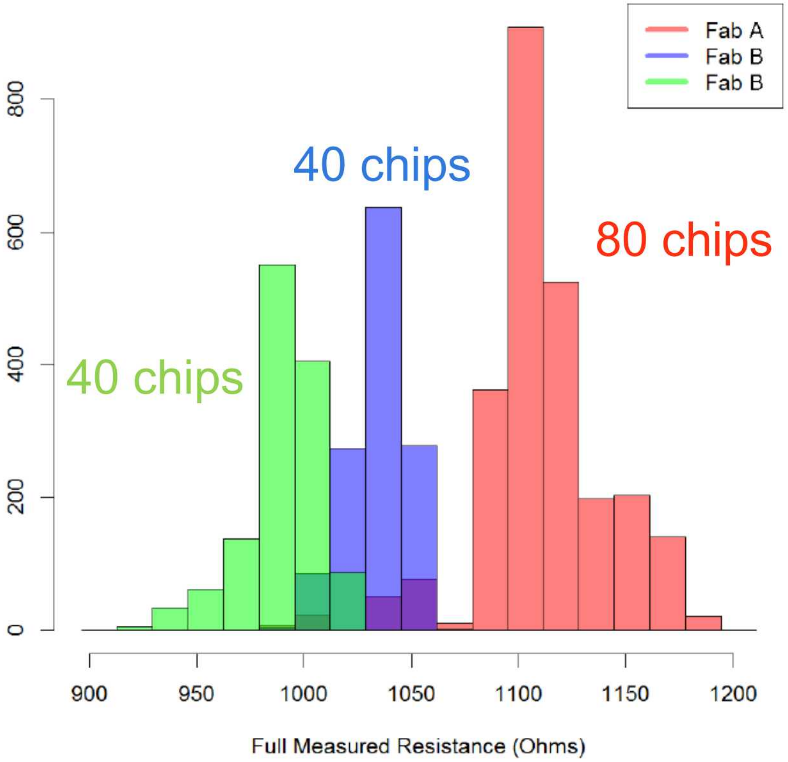
Hofker et al., *Radiation Effects* 24, 223-231 (1975). | Bohm & Hofer (2013).

Quality of PUF Noise Sources

- Recall: Keys should be independently, identically distributed (IID)

FORAB chip (350 nm)





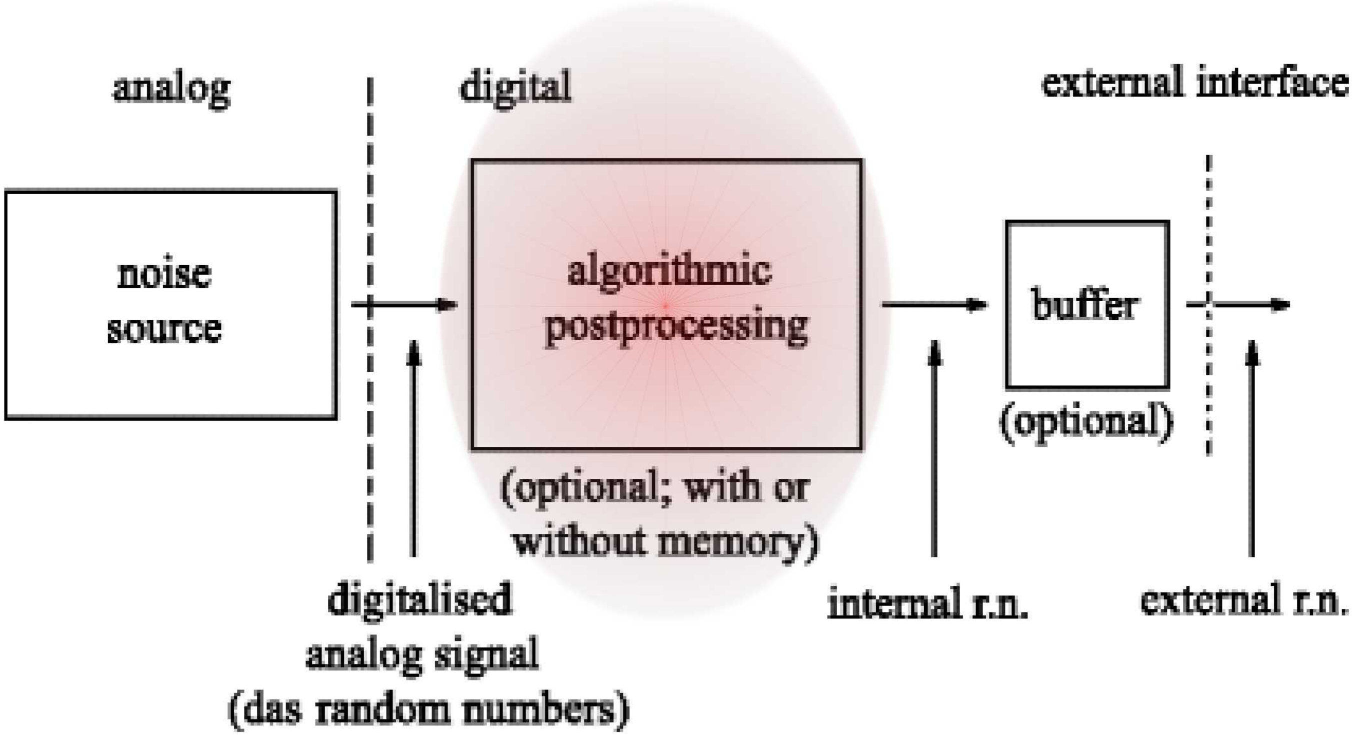
- Resistors: n/p-channel, M1-M4 vias, poly-Si interconnects
  Capacitors: integrating oscillators
  Ring oscillators

- Source of randomness is dependent on fab and lot
  Source of randomness is ~ Gaussian distributed
  NOT IID

Helinski et al., HOST 2016.

Key Generation with PUFs

- Keys should be *n*-bits long depending on security requirements
- Keys should be independently, identically distributed (IID)
- Keys should remain the same throughout the duration of use



analog
digital
external interface
noise source
algorithmic postprocessing
buffer
(optional)
(optional; with or without memory)
digitalised analog signal (das random numbers)
internal r.n.
external r.n.

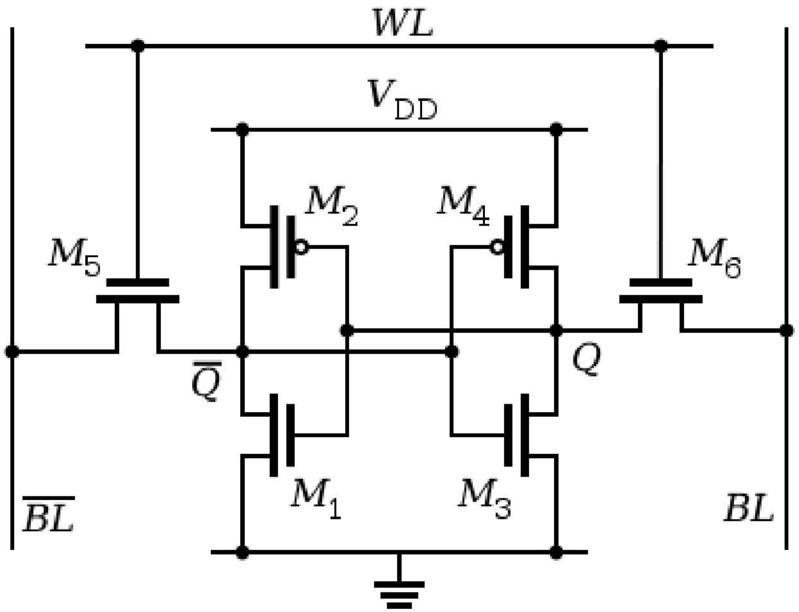
Koc (ed.), *Cryptographic Engineering*, DOI: 10.1007/978-0-387-71817-0, Springer-Verlag (2009).

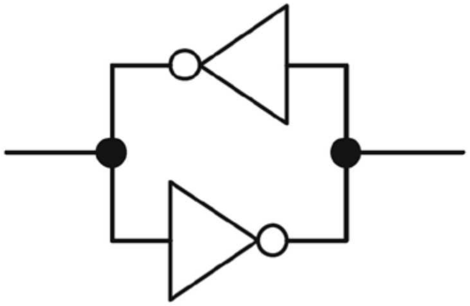
Randomness Extractors

- OK if source is not IID, as long as it's a random variable (**seed**)

  Randomness extractors transform value to IID

  Recall: e.g., SRAM cell is a non-linear feedback circuit





  - On power-up, satisfies conditions for an autonomous, chaotic circuit

    1) 1+ non-linear elements

    2) 1+ locally active resistors

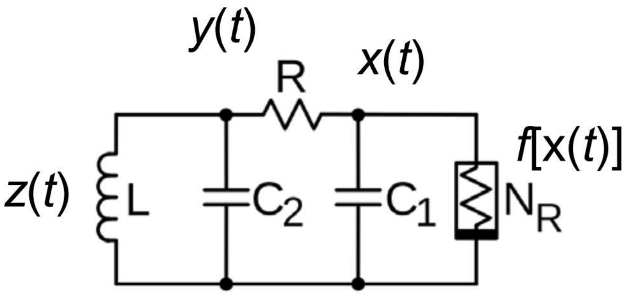
    3) 3+ energy storage elements

Randomness Extractors

- OK if source is not IID, as long as it’s a random variable (**seed**)

  Randomness extractors transform value to IID

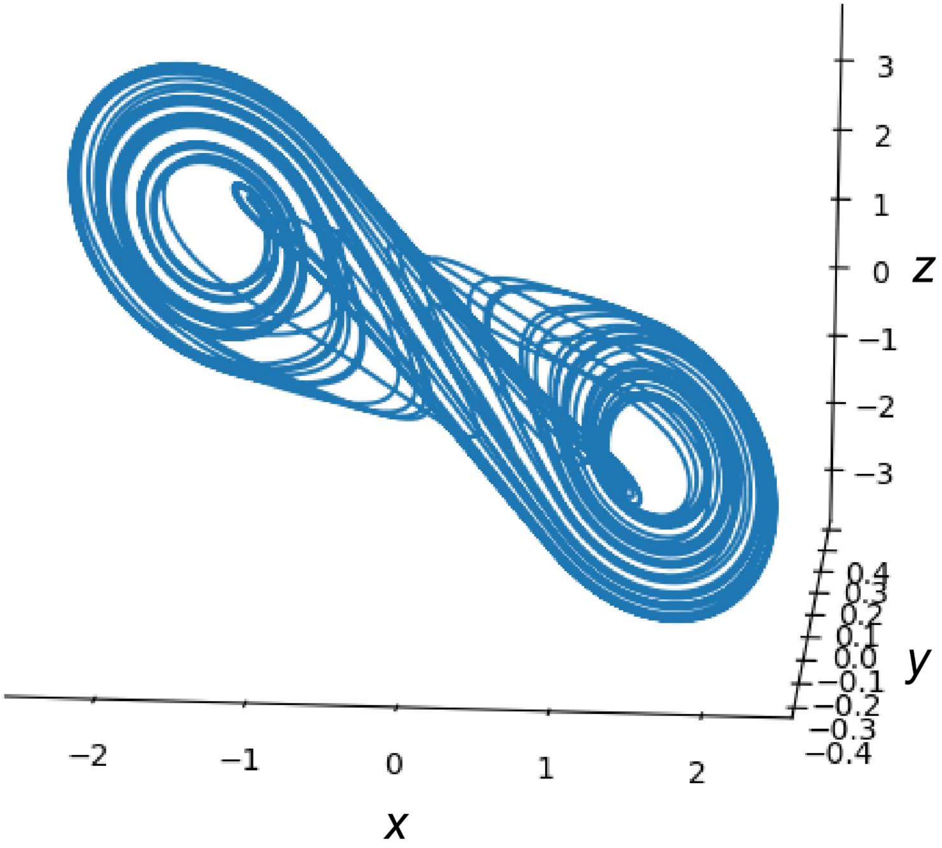
  Chaotic Circuit: Chua’s Circuit, a model chaotic circuit



$$\frac{dx}{dt} = \alpha[y - x - f(x)],$$

$$RC_2\frac{dy}{dt} = x - y + Rz,$$

$$\frac{dz}{dt} = -\beta y.$$



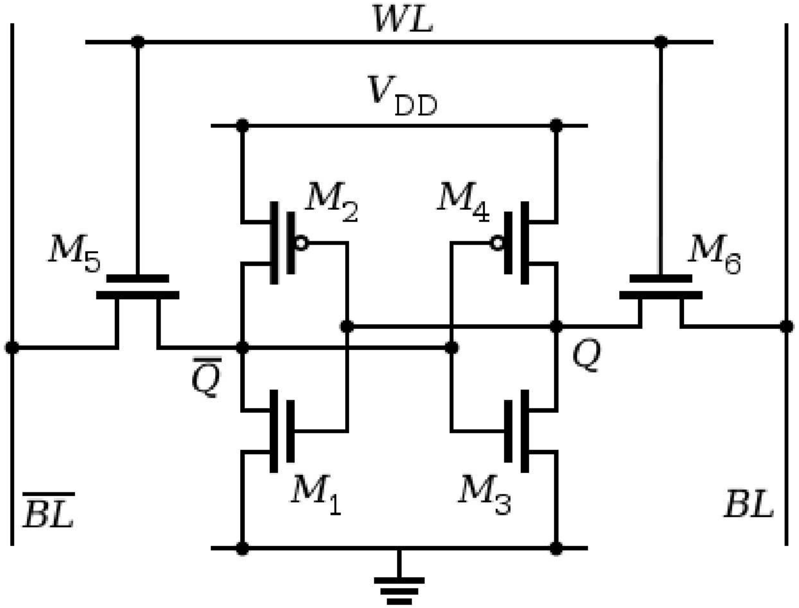
Matsumoto, "A Chaotic Attractor from Chua's Circuit“, IEEE Trans. Circuits and Systems. 12, 1055–1058 (1984).

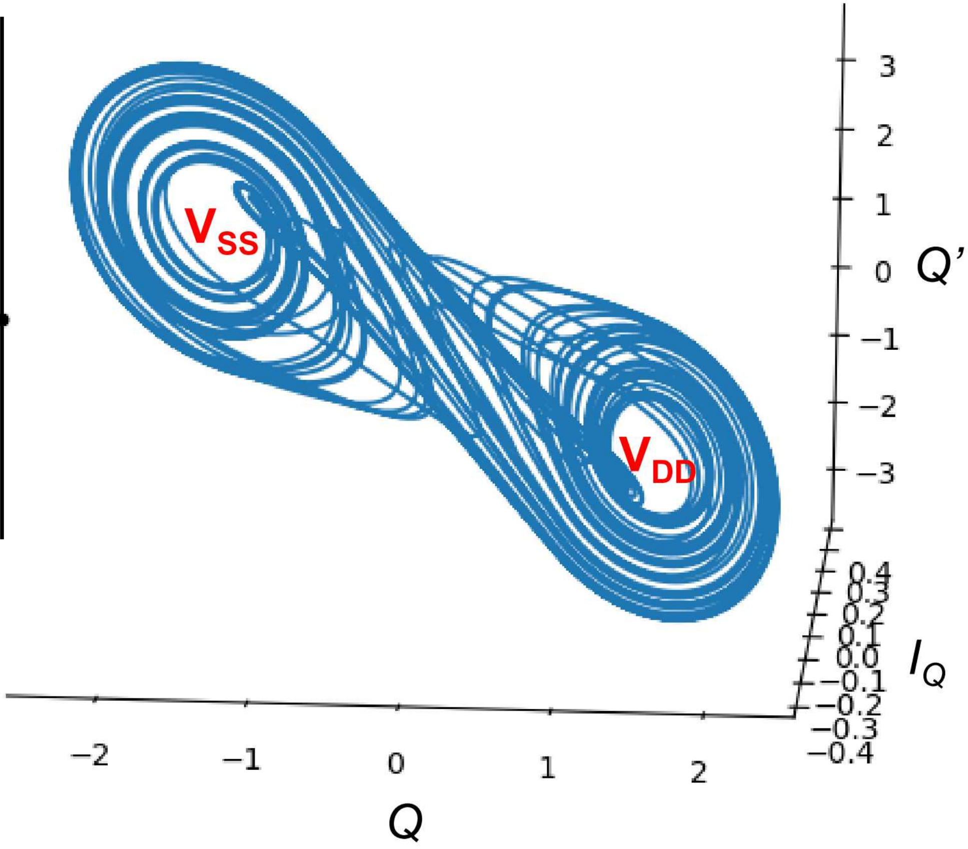
Randomness Extractors

- OK if source is not IID, as long as it’s a random variable (**seed**)

  Randomness extractors transform value to IID

  Chaotic Circuit: SRAM as a chaotic circuit





- Time-dependent output highly sensitive to parameters and starting conditions

  Prone to operational noise

Clark et al., IEEE Trans. VLSI Systems 26, 2027–2037 (2018).

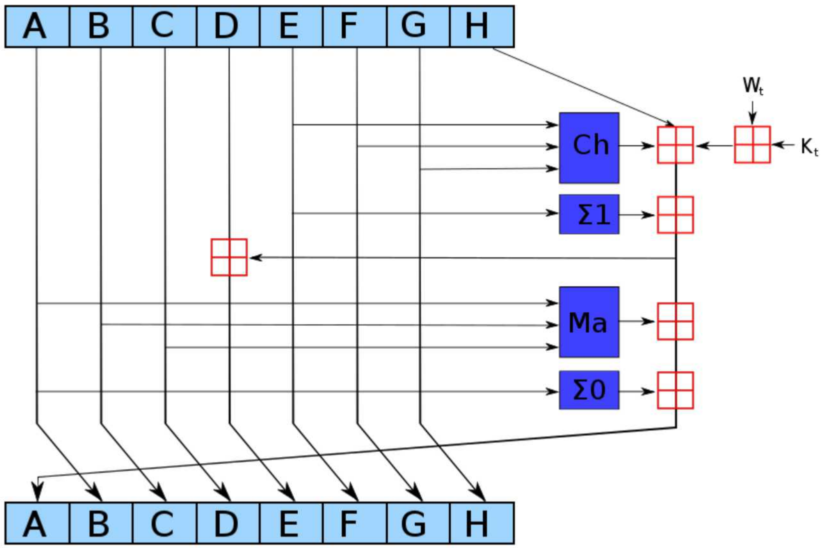
Randomness Extractors

- OK if source is not IID, as long as it's a random variable (**seed**)

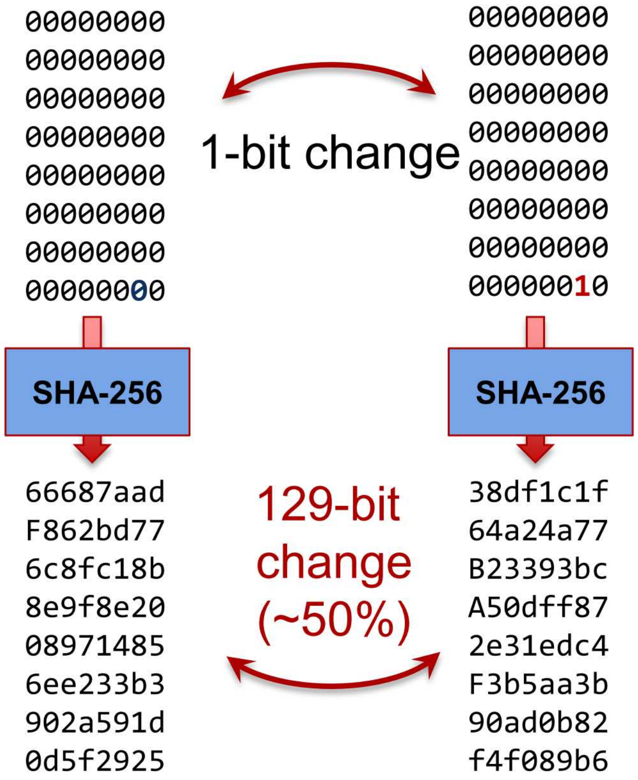
  Randomness extractors transform value to IID

  Algorithmic Extractors: Hash functions, AES S-box

SHA-256 (x64 Rounds)



$$\mathrm{Ch}(E,F,G) = (E \land F) \oplus (\neg E \land G)$$
$$\mathrm{Ma}(A,B,C) = (A \land B) \oplus (A \land C) \oplus (B \land C)$$
$$\Sigma_0(A) = (A \ggg 2) \oplus (A \ggg 13) \oplus (A \ggg 22)$$
$$\Sigma_1(E) = (E \ggg 6) \oplus (E \ggg 11) \oplus (E \ggg 25)$$



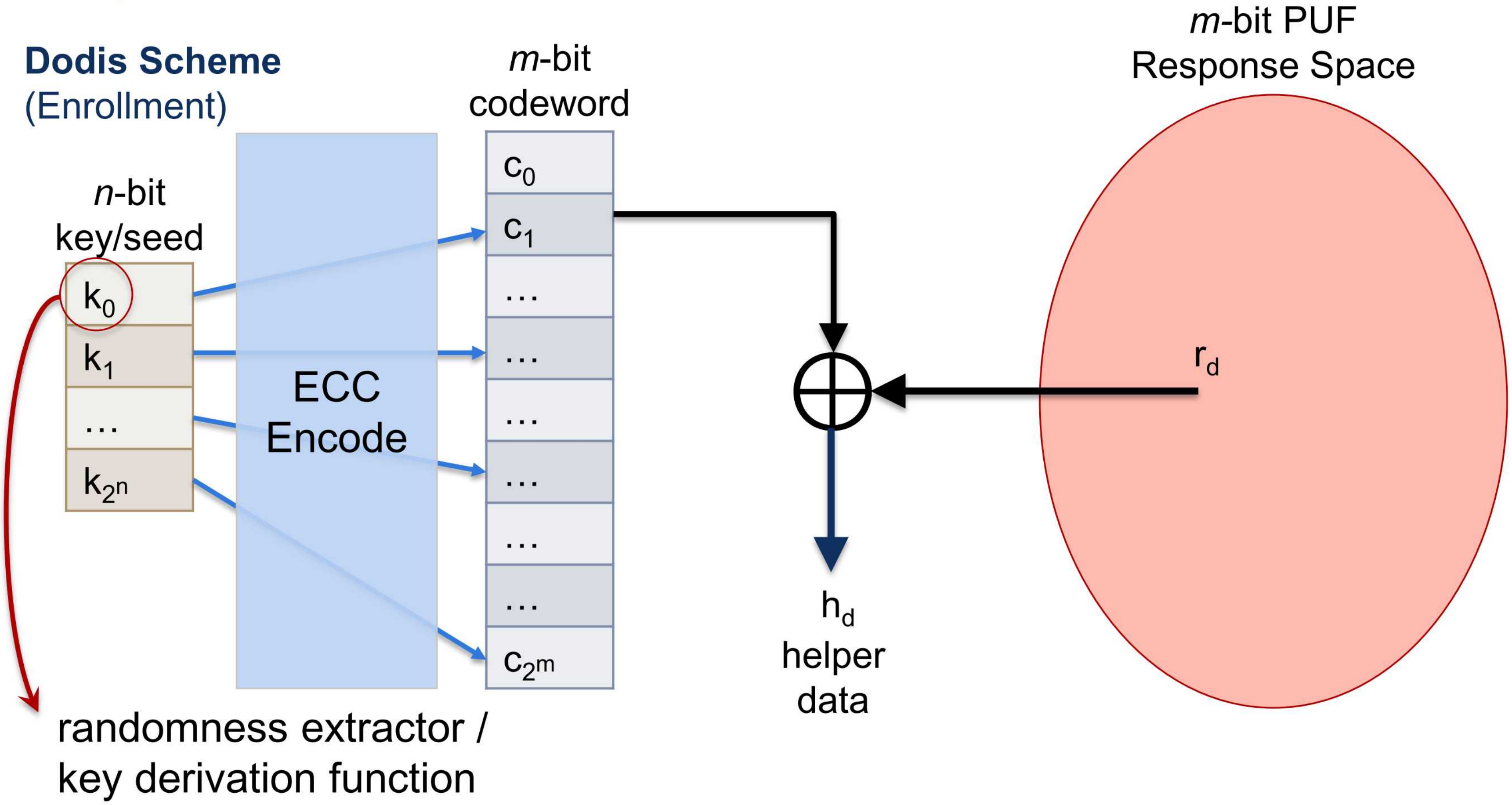
```
00000000        00000000
00000000        00000000
00000000        00000000
00000000        00000000
00000000        00000000
00000000        00000000
00000000        00000000
00000000        00000010

66687aad        38df1c1f
F862bd77        64a24a77
6c8fc18b        B23393bc
8e9f8e20        A50dff87
08971485        2e31edc4
6ee233b3        F3b5aa3b
902a591d        90ad0b82
0d5f2925        f4f089b6
```

- Hashes designed to amplify changes in input: **Prone to operational noise**

Fuzzy Extractors

- Randomness extractors sensitive to operational noise

  Fuzzy extractors add some reliability back

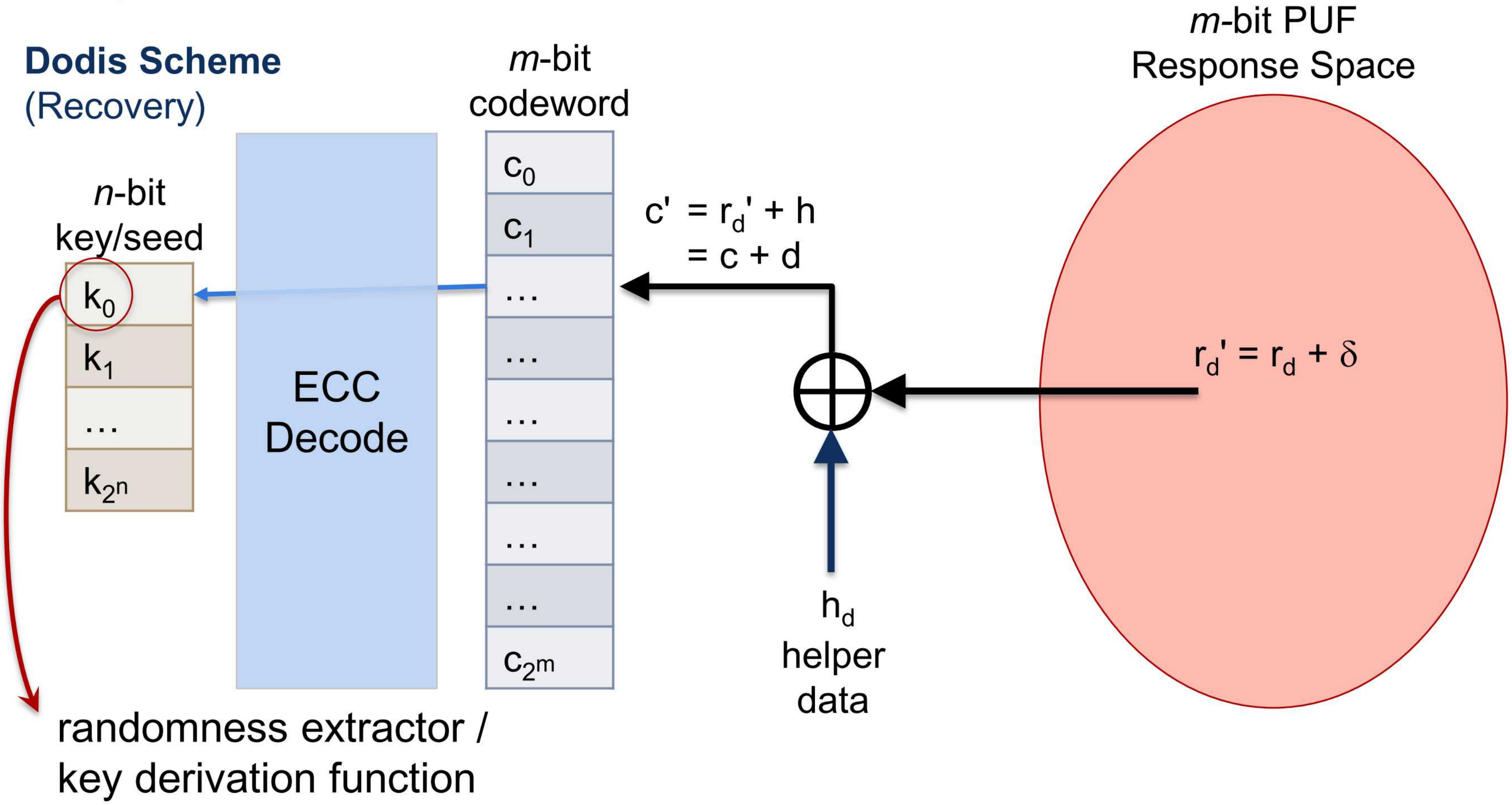


Dodis et al., SIAM J. Computing 38(1), 97—139 (2008).

Fuzzy Extractors

- Randomness extractors sensitive to operational noise

  Fuzzy extractors add some reliability back

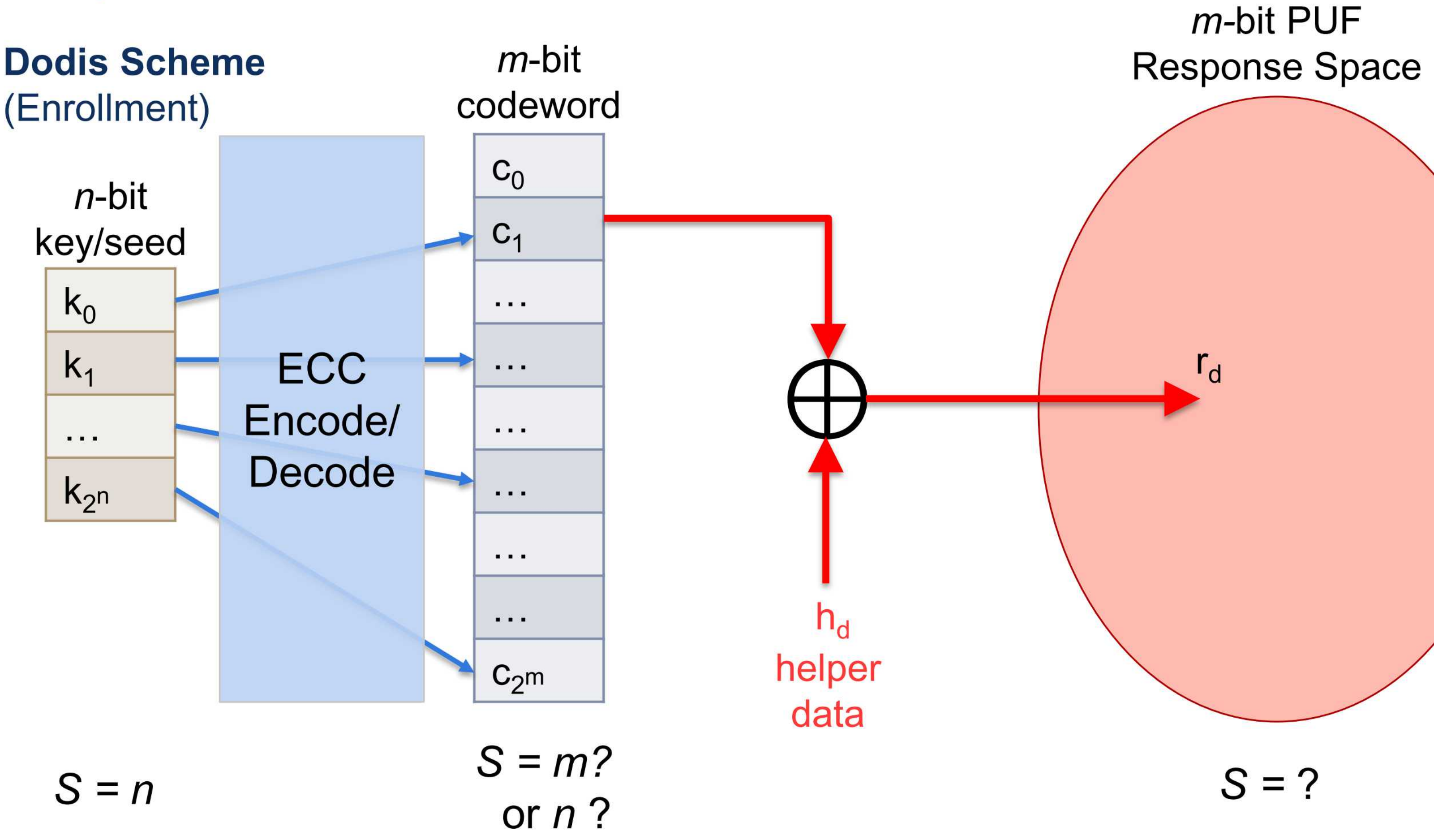


- **PUFs serve as a device-specific one-time pad, hiding sensitive information**

Fuzzy Extractors

- Randomness extractors sensitive to operational noise

  Fuzzy extractors add some reliability back

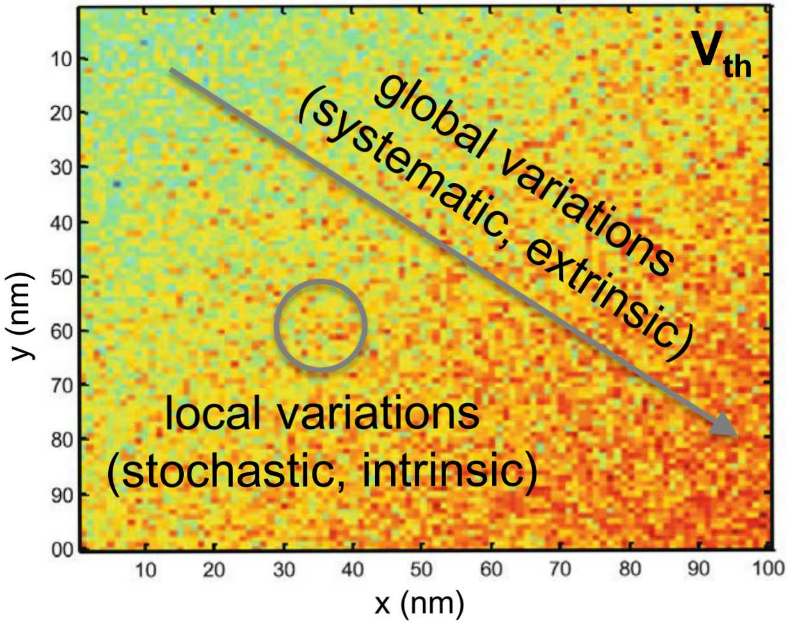


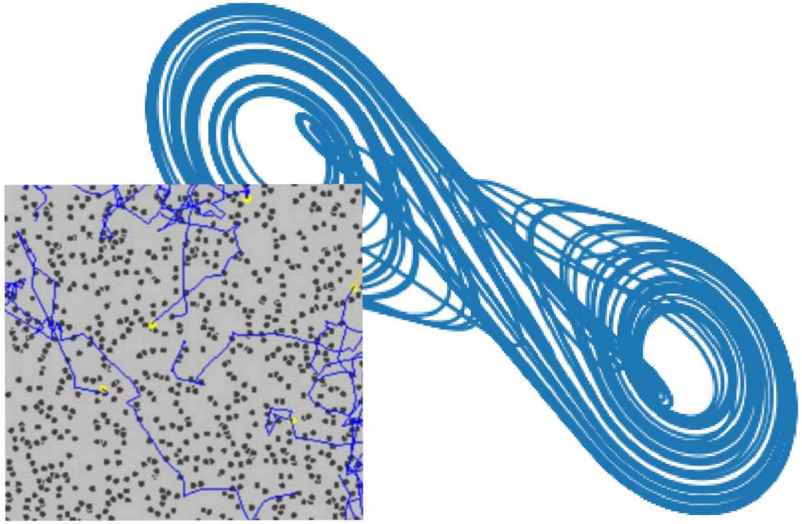
- **Caution: Scheme only as secure as your least entropic element (PUF?)**

Summary

- PUFs leverage manufacturing variations in ICs as digital fingerprints for keys or seeds.

- “PUFs are now a secure alternative [for] secret keys…” (Wikipedia)





- PUFs are likely stochastic and chaotic, but exact sources and distributions TBD.

- PUFs should be implemented and used with extreme care.