TELECOM ParisTech

Institut Mines-Télécom

Reliability and Entropy of Delay PUFs:

A Theoretical Analysis

Alexander Schaub, Jean-Luc Danger, Sylvain Guilley, Olivier Rioul

<firstname.lastname@telecom-paristech.fr>

Physically Unclonable Functions (PUFs)

Motivating Examples

GAMING NINTENDO

Nintendo's Switch can be hacked to run custom apps and games

30

A nightmare

QUICK LINKS: Salted Hash · Reviews · Video · Newsletters · Daily Dashboard · CSO50 Awards · Security Smart · Resources/White Papers · Job Search

CSO FROM IDG

Home > Access Control > Passwords

INSIDER FEATURE

1.4B stolen passwords are free for the taking: What we know now

ıkedIn password breach, and others like it, are still paying dividends for criminals

M. Porup
Writer, CSO MAR 28, 2018 2:20 PM PT

Twitter Admits Recording Plaintext Passwords in Internal Logs, Just Like GitHub

By Catalin Cimpanu May 3, 2018 05:15 PM 1

List of data breaches

From Wikipedia, the free encyclopedia

For a broader coverage related to this topic, see Data breach.

This is a list of **data breaches**, using data compiled from various sources, including press reports, government news releases and mainstream news articles. The list includes those involvi records, although many more smaller breaches occur continually. Breaches of large organizations where the number of records is still unknown are also listed. The various methods used the most common.

Most breaches occur in North America. It is estimated that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.[1][2] It records were exposed as a result of data breaches.[3] Vigilante.pw lists over 2,100 websites which have had their databases breached, containing over 2 billion user entries in total.

Entity	Year	Records	Organization type	Method	Sources
Yahoo	2013	3,000,000,000	web	hacked	[255][256]
Yahoo	2014	500,000,000	web	ha	
Friend Finder Networks	2016	412,214,295	web	pc	
Massive American business hack including 7-Eleven and Nasdaq	2012	160,000,000	financial	ha	
Adobe Systems	2013	152,000,000	tech	ha	
Under Armour	2018	150,000,000	Consumer Goods	ha	
eBay	2014	145,000,000	web	ha	
Equifax	2017	143,000,000	financial, credit reporting	pc	
Heartland	2009	130,000,000	financial	ha	

175,000 IoT cameras can be remotely hacked thanks to flaw, says security researcher

Researchers have found that it's trivial to remotely access one brand of security camera.

By Danny Palmer | July 31, 2017 -- 16:01 GMT (17:01 BST) | Topic: Security

TELECOM ParisTech

Physically Unclonable Functions (PUFs)
PUF Definition

Definition (strong PUF)

Physical device defined by:

- Input: challenge bit-string $C \in \{0,1\}^n$
- Output: bit response $\mathcal{P}(C) \in \{0,1\}$.

The device should not be clonable (physically and mathematically).

Note

Real PUFs are not deterministic and subject to

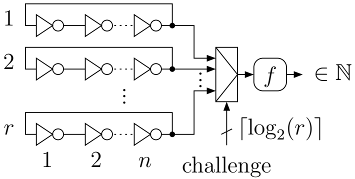
- noise
- aging
- etc.

Types of Unclonable Functions

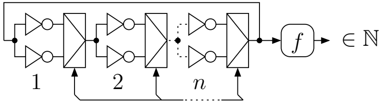
- SRAM PUF
- Delay PUFs:
  - Arbiter PUF
  - Ring oscillator
  - RO-sum PUF
  - Loop-PUF
  - ...
- Optical PUFs
- Glitch PUF
- VIA PUF

Types of Unclonable Functions
Zoom on Delay PUFs

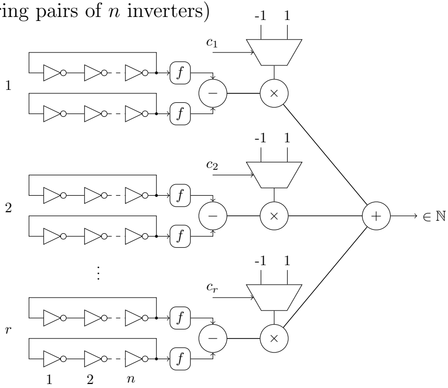
Ring-oscillator PUF
(r rings of n inverters)



Loop-PUF
(with n inverters)



RO-sum PUF
(r ring pairs of n inverters)



Modelisation of Delay PUFs

Ideal (noiseless) output: $\mathcal{P}(C) = \text{sign}(\delta_C)$.
For a PUF subject to additive noise Z:

$$\mathcal{P}(C) = \text{sign}(\delta_C + Z)$$

where:

- Static randomness: $\delta_C \sim \mathcal{N}(0, \Sigma^2)$
- Dynamic randomness: $Z \sim \mathcal{N}(0, \sigma^2)$

$$SNR = \frac{\Sigma^2}{\sigma^2}$$

Independency Hypothesis

$\mathcal{P}(C)$ independent for different challenges C
(made possible by restricting challenges).

Reliability
BER: Definition and Expression

Definition

BER (bit error rate): probability that the outcome differs from the ideal output:

$$\mathrm{BER} = \mathbb{P}_Z[\mathrm{sign}(\delta_C + Z) \neq \mathrm{sign}(\delta_C)]$$

Averaged over the static randomness:

$$\widehat{\mathrm{BER}} = \mathbb{E}_{\delta_C}[\mathrm{BER}]$$

Theorem (Closed Form Expressions for BER)

$$\mathrm{BER} = \frac{1}{2}\,\mathrm{erfc}\left(\frac{|\delta_C|}{\sigma\sqrt{2}}\right)$$

$$\widehat{\mathrm{BER}} = \frac{1}{\pi}\arctan\left(\frac{1}{\sqrt{\mathrm{SNR}}}\right)$$

BER Expression Proofs

Proof (BER)..

Assume $\delta_C > 0$ (symmetrical proof for $\delta_C < 0$).

$$\mathbb{P}[\delta_C + Z < 0] = \mathbb{P}[Z < -\delta_C] = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{-\delta_C} e^{\frac{-z^2}{2\sigma^2}} dz = \frac{1}{2}\,\mathrm{erfc}(\frac{\delta_C}{\sigma\sqrt{2}}) \qquad \square$$

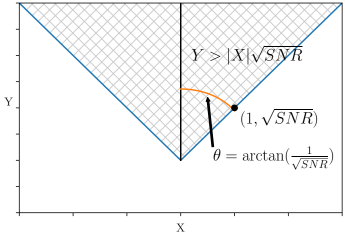
Proof (Averaged BER)..

$\mathbb{P}[\mathrm{sign}(\delta_C + Z) \neq \mathrm{sign}(\delta_C)] = \mathbb{P}[Z > |\delta_C|]$.

But

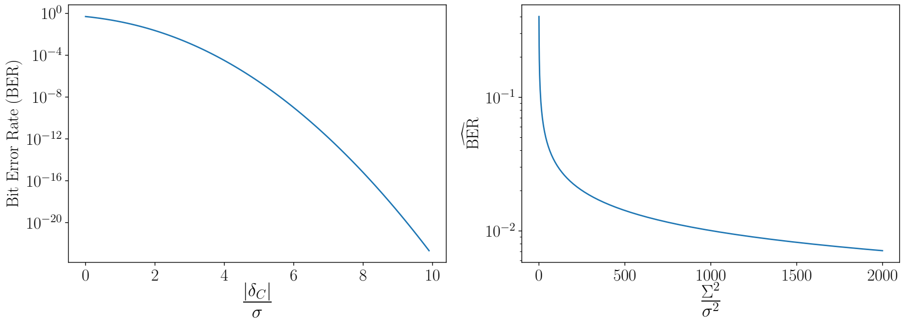
$Z > |\delta_C| \Leftrightarrow \frac{Z}{\sigma} > \frac{|\delta_C|}{\Sigma}\frac{\Sigma}{\sigma} \Leftrightarrow Y > |X|\sqrt{SNR}$

where $X, Y \sim \mathcal{N}(0, 1)$ $\square$

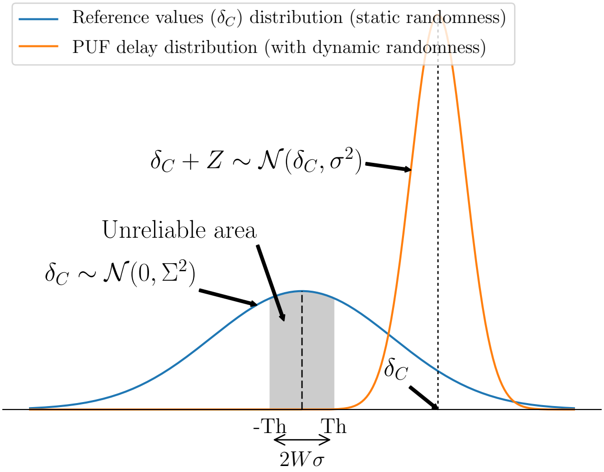


Reliability

Evolution of the BER



Dynamic vs Static Randomness
An Illustration



Reliability Improvement : Filtering

- Discard "unstable" bits
- Unstable: $|\delta_C| < \mathrm{Th} = W\sigma$
- Tradeoff: improves reliability but reduces number of output bits

$$W = \text{relative threshold proportion} = \frac{\mathrm{Th}}{\sigma}$$

Reliability Improvement

Closed-Form Expression for Filtered Output

Filtered BER depends on W as well as the SNR:

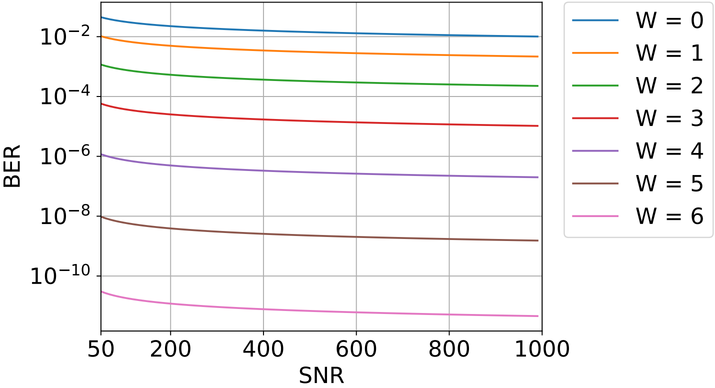
Theorem (BER After Filtering)

$$\widehat{\mathrm{BER}}_{filt} = \frac{2}{\mathrm{erfc}(\frac{W}{\sqrt{2}\cdot\sqrt{\mathrm{SNR}}})}\left(T(W, \frac{1}{\sqrt{\mathrm{SNR}}}) + \frac{1}{4}\,\mathrm{erf}(\frac{W}{\sqrt{2}\cdot\sqrt{\mathrm{SNR}}})(\mathrm{erf}(\frac{W}{\sqrt{2}}) - 1)\right)$$

where T is Owen's T-function:

$$T(h, a) = \frac{1}{2\pi}\int_0^a \frac{e^{-\frac{1}{2}h^2(1+x^2)}}{1+x^2}dx.$$

Reliability Improvement : Summary
BER as a function of *W* and SNR



BER mainly depends on W, less sensitive on the SNR.

Reliability Improvements
Entropy Loss

Assuming n independent challenge responses, entropy $H = n$.

After filtering, the remaining entropy is the number of "stable" bits:

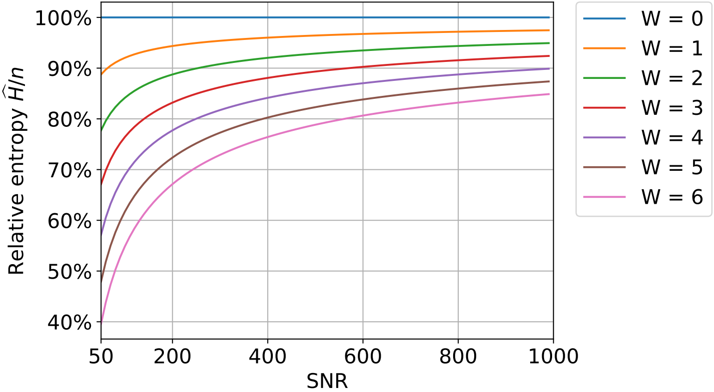
Theorem (Entropy After Filtering)

Average (over static randomness) entropy for n delay elements:

$$\widehat{H(n, W)}_{SNR} = n \cdot \mathrm{erfc}\left(\frac{W}{\sqrt{2\mathrm{SNR}}}\right).$$

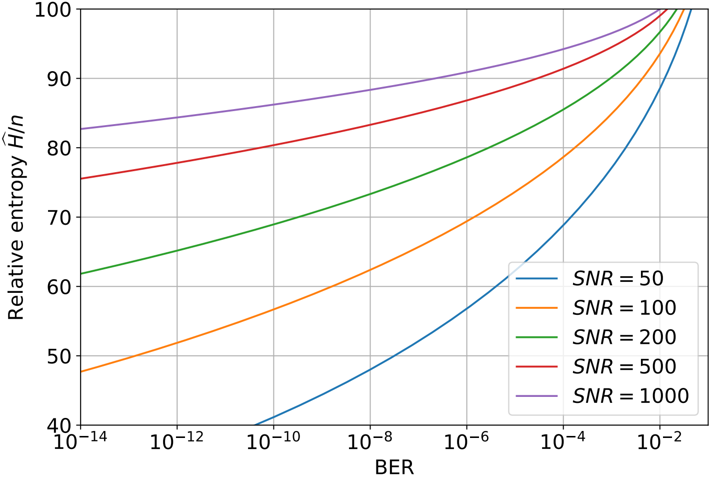
Reliability Improvements

Entropy Loss Figure



High number of rejected output bits for small SNR.

Conclusion: Entropy/BER Tradeoff After Filtering



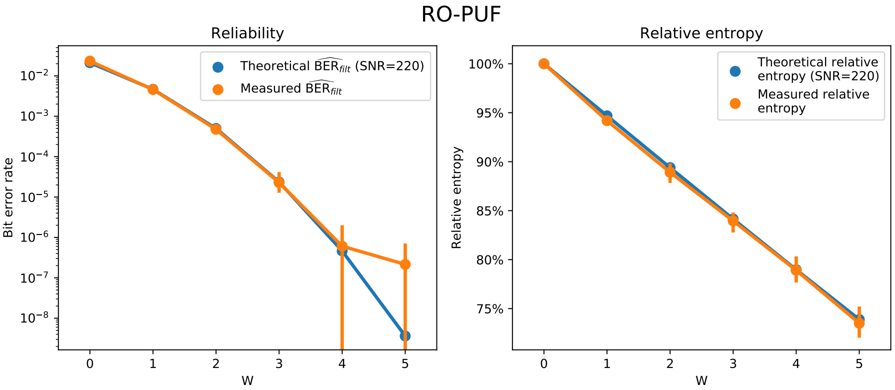
Is our Static/Dynamic Gaussian Model Valid ?

$\Longrightarrow$ Experimental validation needed !

Experimental setup:

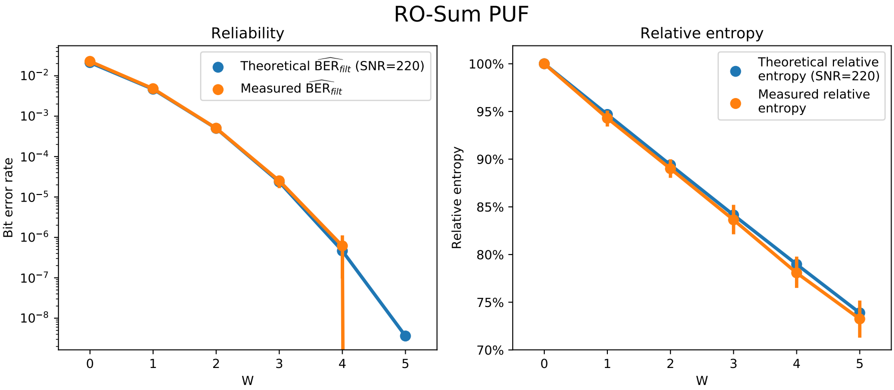
PUF type	Challenge restriction	Evaluation
Ring oscillator	Pairs of independent oscillators	Difference of two delays
RO-sum PUF	Orthogonal challenges	Sum/difference of 48 delays
Loop-PUF	Orthogonal challenges	Native PUFs

Results - Ring Oscillator PUF



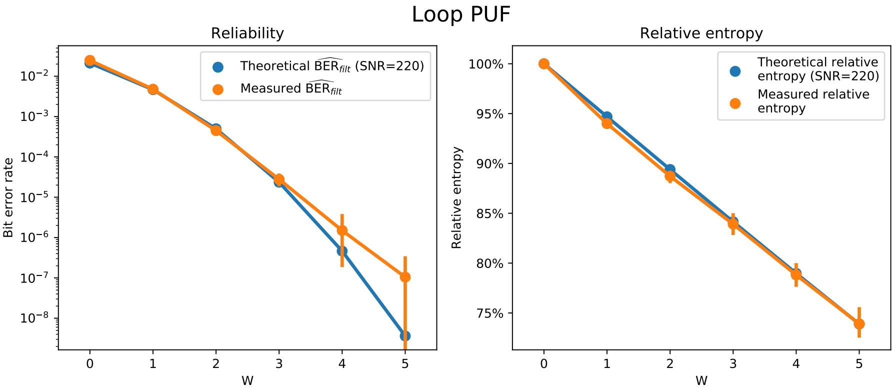
Rejected output bits as expected, too high BER.

Results - RO-sum PUF



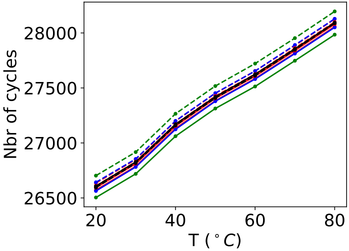
BER and relative entropy as expected.

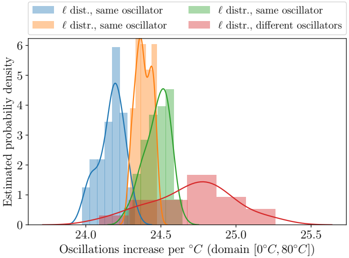
Results - Loop PUF



Rejected output bits as expected, too high BER.

Environmental Effects
Temperature Dependency





Temperature dependency

Modelisation:

$$\mathcal{P}_\theta(C) = \delta_C + Z + \ell\theta$$

θ: temperature difference

Temperature coefficient

Modelisation:

$$\ell \sim \mathcal{N}(0, \sigma_\theta^2)$$

Temperature Dependency

Temperature-Dependent BER

Definition

Temperature-dependent BER:

$$\widehat{BER_\theta} = \mathbb{P}[\text{sign}(\delta_C + Z + \ell\theta) \neq \text{sign}(\delta_C)]$$

Theorem (BER Closed Form Expression)

$$\widehat{BER_\theta} = \frac{1}{\pi} \arctan\left(\frac{\sqrt{\sigma^2 + \theta^2\sigma_\theta^2}}{\Sigma}\right)$$

*For **average** BER, change in temperature equivalent to reduction in SNR.*

Wrap up

- A novel theoretical **modelization** for Delay-PUFs
- Bit **filtering**: **reliability** / **entropy** tradeoff
- Experimental **validation**
- Temperature dependency modelization

Institut
Mines-Télécom

Reliability and Entropy of Delay PUFs:

A Theoretical Analysis

Alexander Schaub, Jean-Luc Danger,
Sylvain Guilley, Olivier Rioul
<firstname.lastname@telecom-paristech.fr>