Rényi Entropy Estimation for Secure Silicon Fingerprints

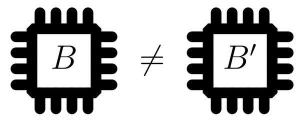
Alexander Schaub, Olivier Rioul, Sylvain Guilley, Jean-Luc Danger, Joseph J Boutros

Rényi Entropy Estimation for Secure Silicon Fingerprints

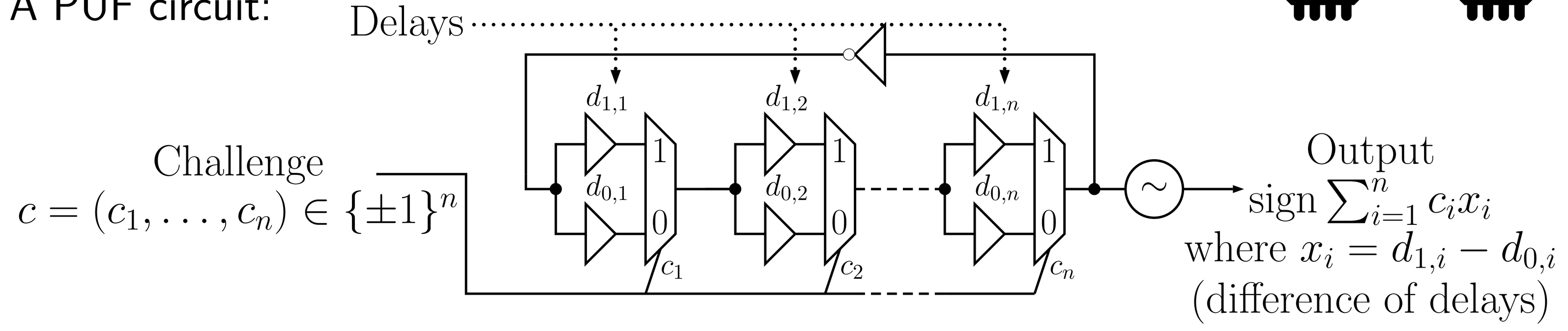
Alexander Schaub[1], Olivier Rioul[1], Sylvain Guilley[1,2], Jean-Luc Danger[1,2] & Joseph J. Boutros[3]

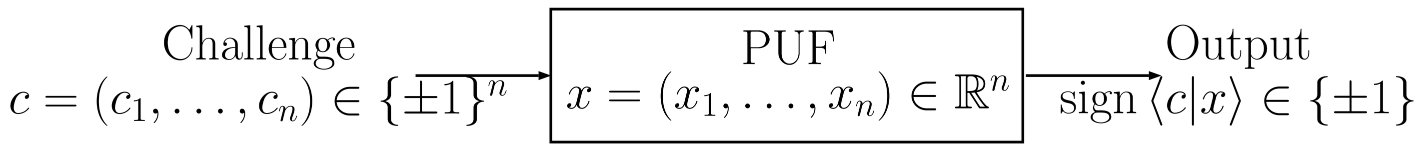
[1] LTCI, Télécom Paris, Institut Polytechnique de Paris, France, [2] Secure-IC S.A.S., France, [3] Texas A&M University at Qatar, Doha, Qatar

Physically Unclonable Function (PUF)



A PUF circuit:





The PUF parameter x is **uncontrollable**: it depends on the manufacturing process and varies from one circuit to another ("static randomness").

x : outcome of an **i.i.d random vector** $X = (X_1, \dots, X_n)$ where $X_i \sim -X_i$.

The PUF behavior depends on a **challenge code**

$$\mathcal{C} = \{c^1, \dots, c^M\}$$

that defines the PUF output (**silicon fingerprint**)

$$B = (B_1, \dots, B_M) \text{ where } B_j = \operatorname{sign} \langle c^j | X \rangle .$$

Motivation

Given a PUF design:

- **How much randomness** can be extracted from it ? More precisely:
- How **unique** is the generated identifier (collision resistance) ?
- Can a PUF be used to generate a (say) 128-bit **cryptographic key** ?
- How difficult is it to **predict** the PUF response (using machine learning, e.g., SVM) ?

Rényi Entropy as a PUF Security Metric

α-Entropy

$$H_\alpha(B) = \frac{1}{1-\alpha} \sum_{b \in \{\pm 1\}^M} P_B(b)^\alpha$$

Definition	Name	Significance
$H_0(B) = \log \#\mathrm{Supp}(B)$	max-entropy	Number of PUFs
$H_1(B) = H(B)$	Shannon entropy	Probabilistic uncertainty
$H_2(B) = -\log \mathbb{P}(B = B')$, $B \perp\!\!\!\perp B'$	Collision entropy	Resistance to random collisions
$H_\infty(B) = -\log \max_b P_B(b)$	**min-entropy**	**Brute-force resistance**

- $H_\alpha(B_1, \dots, B_M)$ **increases** with M (when adding new challenges to $\mathcal{C}$).
- $\max_{\mathcal{C}} H_\alpha(B) = H_\alpha(n)$ is attained for $M = 2^n$ (all possible challenges).

BTF Theory and Chow Parameters

A PUF with $M = 2^n$ is identified to a

Boolean Threshold Function (BTF)

$$f_x : c \in \{\pm 1\}^n \mapsto \operatorname{sign} \langle c|x \rangle \text{ for a **fixed** } x \in \mathbb{R}.$$

Chow parameters of a BTF

$$\hat{f}_x = \sum_{f_x(c)=1} c \quad \text{(componentwise)} .$$

They **uniquely identify** a boolean threshold function: $\hat{f}_x = \hat{f}_y \implies f_x = f_y$.

Result on the max-entropy

There are at most 2^{n^2} distinct Chow parameters. Hence $H_0(n) < n^2 \quad (\forall n \geq 2)$.

Invariance Under the Signed Permutation Group

Changing the **order** or **signs** of the X_i's does not change P_B.

Signed Permutation Group:

$G_n = S_n \times \{\pm 1\}^n$ acts on $\mathbb{R}^n$:

$$(g \cdot x)_i = s_i x_{\sigma(i)} \text{ where } g = (\sigma, s) \in S_n \times \{\pm 1\}^n.$$

Results on equal probabilities

- The action of G_n preserves probabilities: $\mathbb{P}(f_X = f_x) = \mathbb{P}(f_X = f_{g \cdot x})$
- Hence all PUFs in $\mathrm{Orb}(f_x) = \{f_{g \cdot x} \mid g \in G_n\}$ have the same probability.

Results on the orbit size

- The action of G_n preserves Chow parameters: $\hat{f}_{g \cdot x} = g \cdot \hat{f}_x$
- Hence, using the orbit-stabilizer theorem on $\mathrm{Orb}(f_x)$,

$$\#\mathrm{Orb}(f_x) = \frac{2^n n!}{2^{m_{\hat{f}_x}(0)} \prod_{k \in \mathbb{N}} m_{\hat{f}_x}(k)!} \quad \text{where } m_{\hat{f}_x}(k) = \#\{i : (\hat{f}_x)_i = \pm k\}.$$

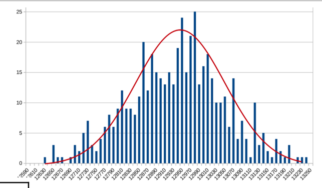
Estimating the PUF Distribution

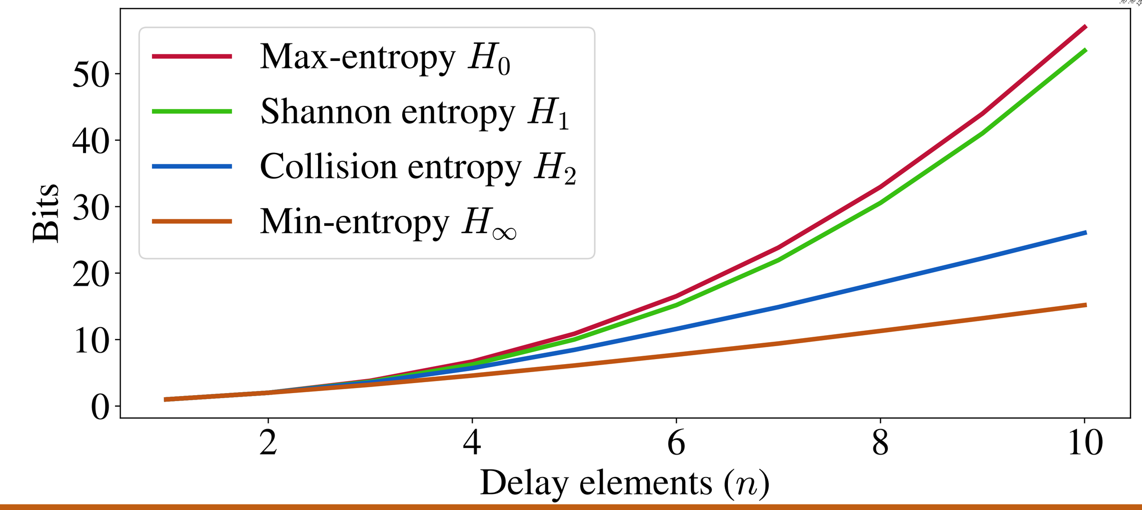
for $i \leftarrow 1$ **to** N **do**
  Generate n realizations $x = (x_1, \dots, x_n)$;
  Take $x \leftarrow |x|$ and sort x to get the orbit leader;
  Compute Chow parameters $\hat{f}_x$;
  Set **count** $[\hat{f}_x] \leftarrow$ **count** $[\hat{f}_x] + 1$;
end
for $c \in$ **count do**
  orbit_size$[c] \leftarrow \frac{2^n n!}{2^{m_c(0)} \prod_{k \in \mathbb{N}} m_c(k)!}$,   **proba**$[c] \leftarrow \frac{\textbf{count}[c]}{N * \textbf{orbit\_size}[c]}$;
end

Simulation interpretation

For any orbit leader f_x, there are **orbit_size**$[\hat{f}_x]$ probabilities equal to **proba**$[\hat{f}_x]$.

Simulation Results for Gaussian X





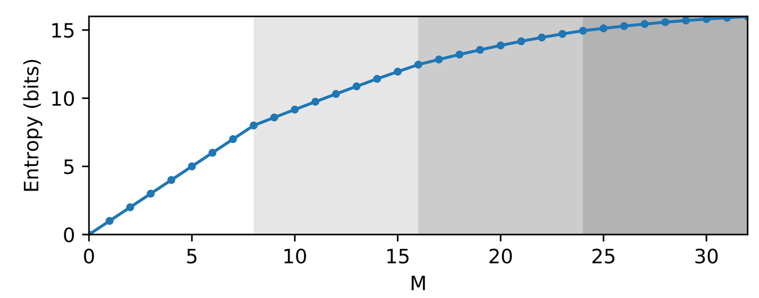
Results with 95 % confidence level

n	Sample size	$H_1(n)$ (bits)	$H_2(n)$ (bits)	$H_\infty(n)$ (bits)
3	N/A	3.6655...	3.5462...	3.2086...
4	N/A	6.2516...	5.7105...	4.5850...
5	10^{10}	$\mathbf{10.014 \pm 1 \cdot 10^{-3}}$	$\mathbf{8.4559 \pm 8 \cdot 10^{-4}}$	$\mathbf{6.1007 \pm 1 \cdot 10^{-4}}$
6	10^{10}	$\mathbf{15.191 \pm 1 \cdot 10^{-3}}$	$\mathbf{11.600 \pm 2 \cdot 10^{-3}}$	$\mathbf{7.7353 \pm 1 \cdot 10^{-4}}$
7	10^{10}	$\mathbf{21.987 \pm 1 \cdot 10^{-3}}$	$\mathbf{14.890 \pm 8 \cdot 10^{-3}}$	$\mathbf{9.4733 \pm 2 \cdot 10^{-4}}$
8	$2 \cdot 10^{10}$	$\mathbf{30.5636 \pm 8 \cdot 10^{-4}}$	$\mathbf{18.55 \pm 3 \cdot 10^{-2}}$	$\mathbf{11.3022 \pm 2 \cdot 10^{-4}}$
9	$2 \cdot 10^{10}$	$\mathbf{41.0376 \pm 8 \cdot 10^{-4}}$	$\mathbf{22.2 \pm 2 \cdot 10^{-1}}$	$\mathbf{13.2127 \pm 4 \cdot 10^{-4}}$
10	$3 \cdot 10^{12}$	$\mathbf{53.4738 \pm 1 \cdot 10^{-4}}$	$\mathbf{26.1 \pm 1 \cdot 10^{-1}}$	$\mathbf{15.1900 \pm 1 \cdot 10^{-4}}$

Conclusion and Perspectives

Cryptographic applications require a source of high entropy.
We show how to calibrate PUFs to achieve a given security level:

- Our simulation results suggest that $H_1(n) \approx n^2$ (much greater than n) !
- Exact computation of entropies for higher values of n becomes intractable.
- But in practice, only a subset of all possible challenges is chosen:
  How should we select them to maximize entropy ?



References

[1] Sze-Tsen Hu. *Threshold Logic*. Univ of California Press, 1965.

[2] Olivier Rioul, Patrick Solé, Sylvain Guilley, and Jean-Luc Danger. "On the entropy of physically unclonable functions". In: *ISIT*. 2016, pp. 2928–2932.

[3] Alexander Schaub, Jean-Luc Danger, Sylvain Guilley, and Olivier Rioul. "An improved analysis of reliability and entropy for delay PUFs". In: *Proc. of Euromicro DSD 2018, Prague*.

[4] Alexander Schaub, Olivier Rioul, and Joseph J. Boutros. "Entropy estimation of physically unclonable functions via Chow parameters". In: *57th IEEE Allerton Conference*. 2019, pp. 698–704.

[5] Alexander Schaub, Olivier Rioul, Jean-Luc Danger, Sylvain Guilley, and Joseph J. Boutros. "Challenge codes for physically unclonable functions with Gaussian delays: A maximum entropy problem". In: *Advances in Mathematics of Communications* (2019).

Contact: alexander.schaub@telecom-paris.fr, website: https://perso.telecom-paristech.fr/aschaub