Image-based PUFs for Anti-Counterfeiting

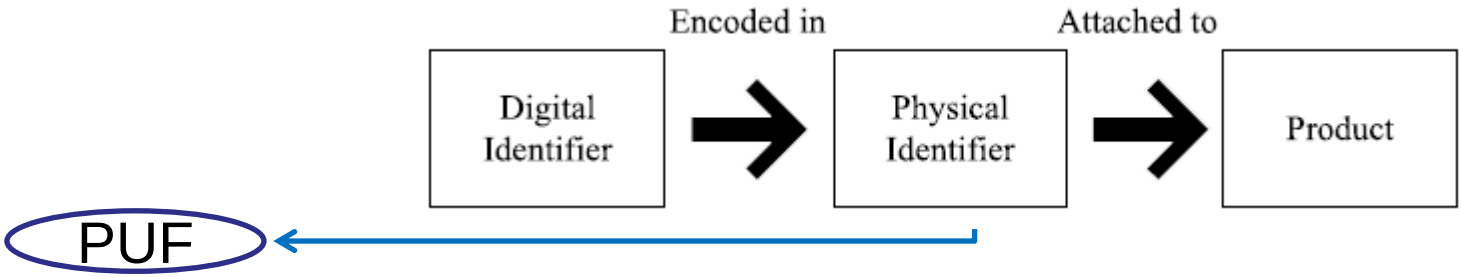
Saloomeh Shariati

Signal Processing Seminar
TELE Lab
Nov 2011

Outline

- Anti-counterfeiting and unclonability
- Image-based PUFs
  - Laser-Written PUF
  - Crystal PUF
- Image-based Physical Function System
  - Image-based Physical Function
  - Image-based Extraction
- Experiments
  - Image-based Extraction
  - Robustness
  - Physical Unclonability

Anti-counterfeiting
State of the art

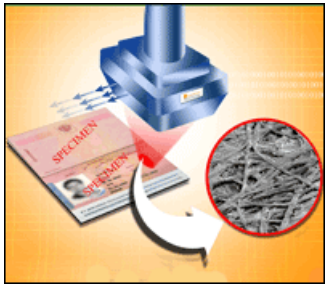


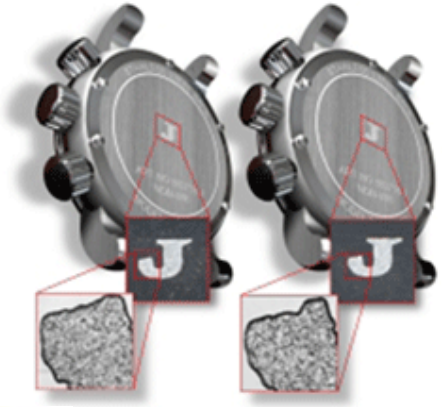
- Two types of physical identifiers:
  - Overt: No need to a specific device
    - Can be easily cloned

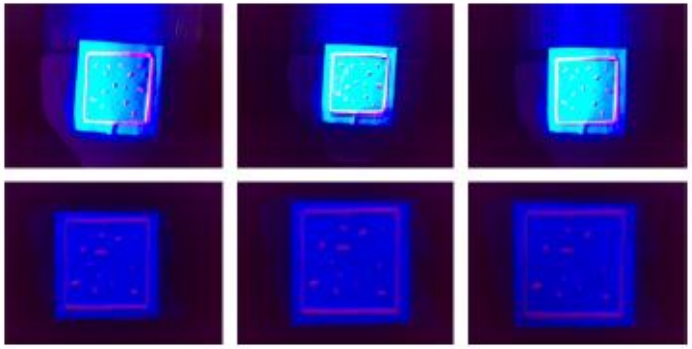
  - Covert: Retrieving digital identifier needs the specific device

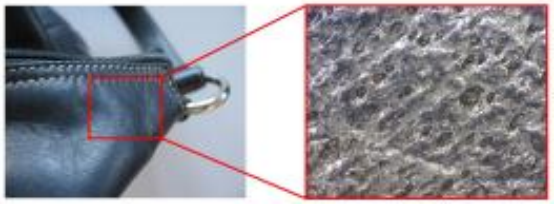
Image-based PUFs

- Using Random features : Hardly-cloneable
- Random features characterized by imaging methods.

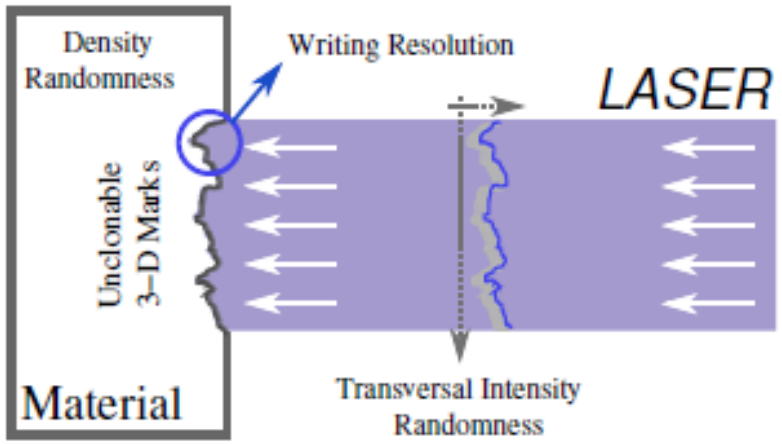






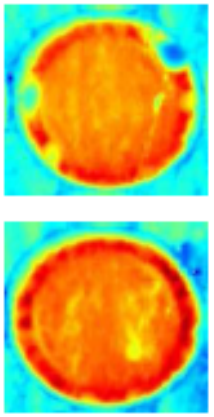


Laser-Written PUF



(a)

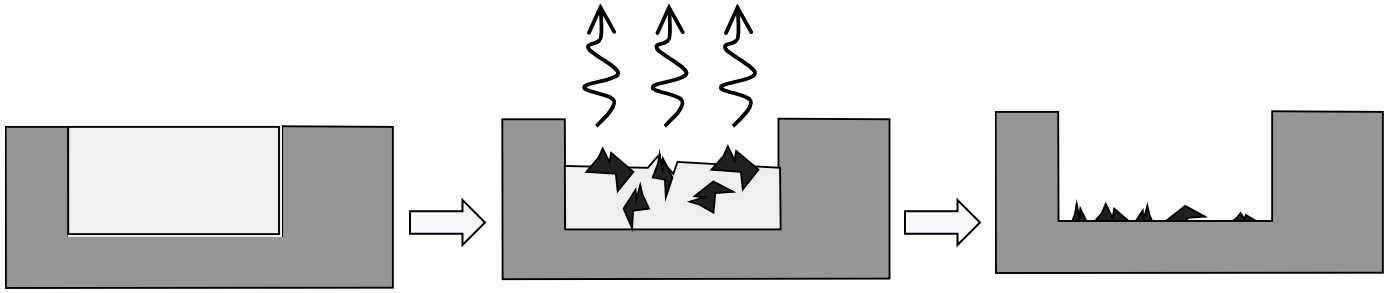
Laser engraving principle

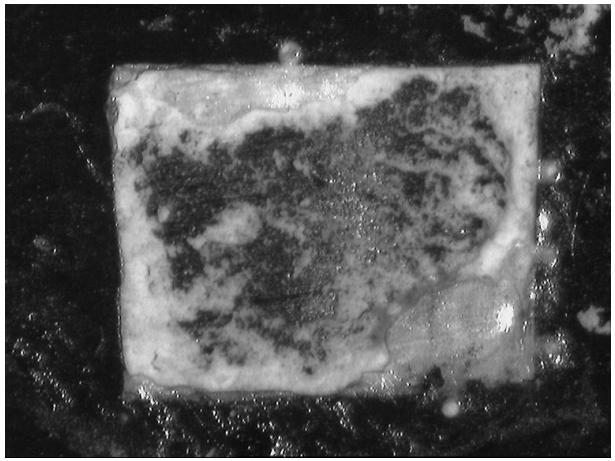


(b)

Two laser marks

Crystal PUF





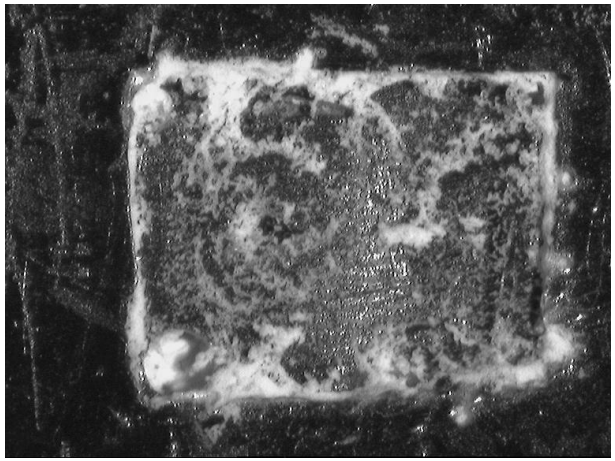
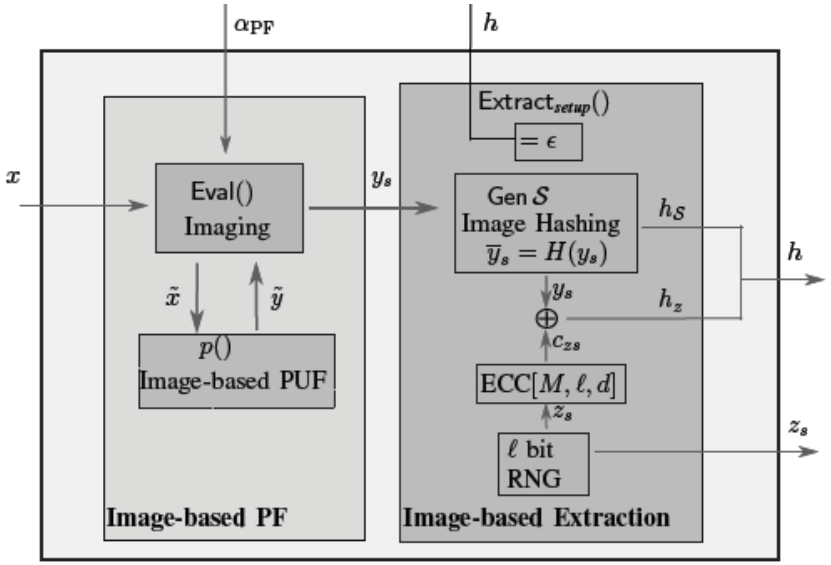
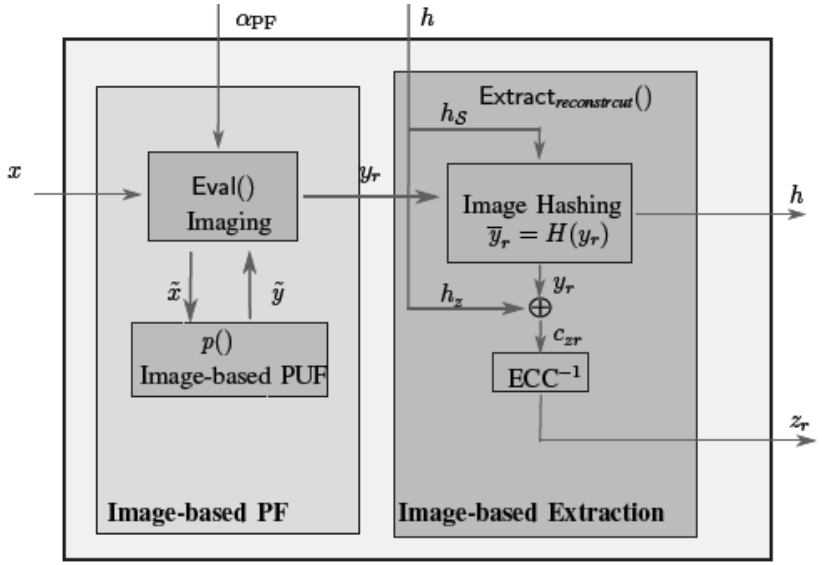


Image-based PF System Model



(a) Setup mode.



(b) Reconstruction mode.

Image-based Extraction: Challenges

- Short Binary identifier instead of a big Image.
- Being robust to observation noise
- Not loosing the randomness present between images.

Image-based Extraction

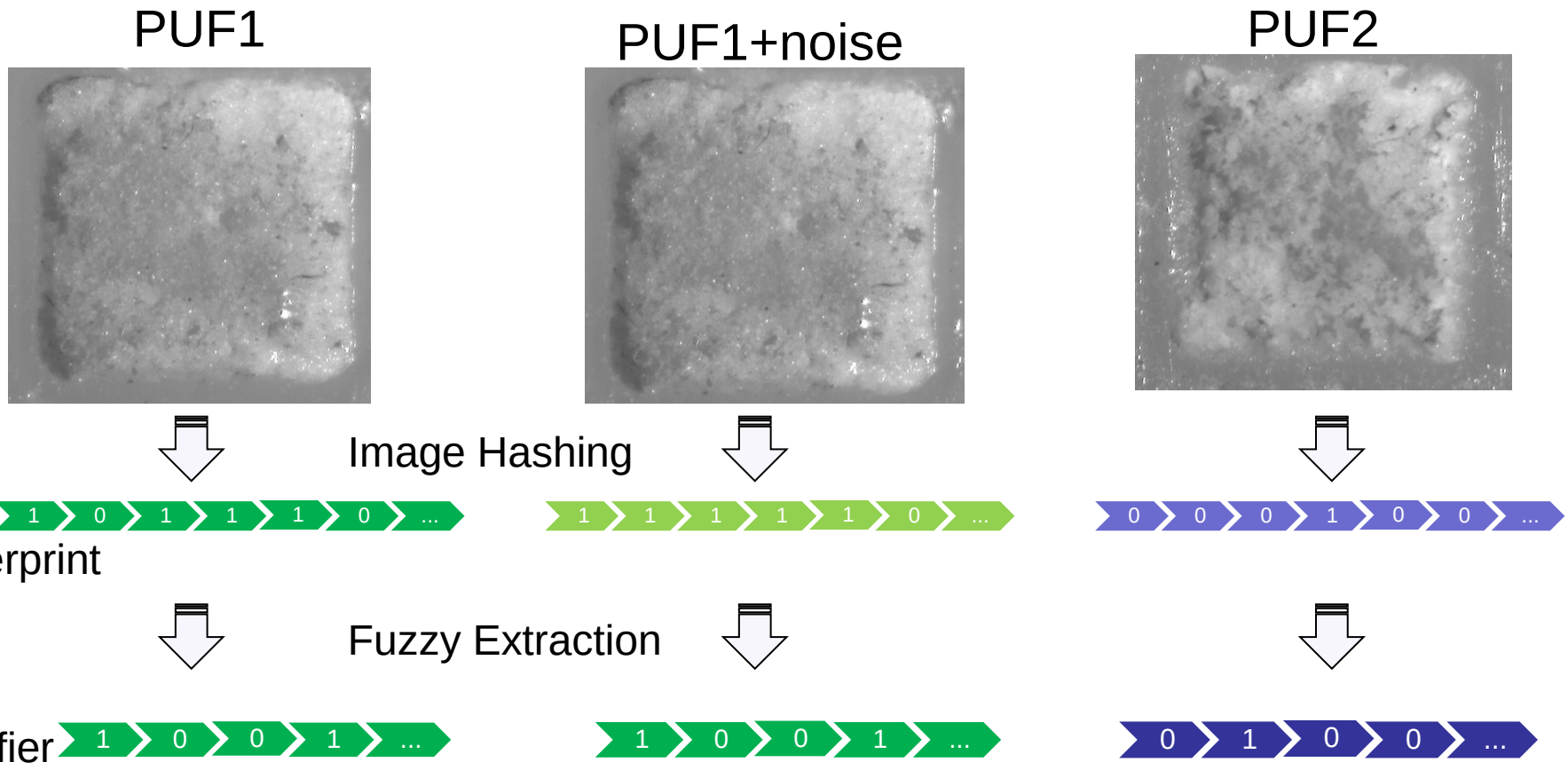
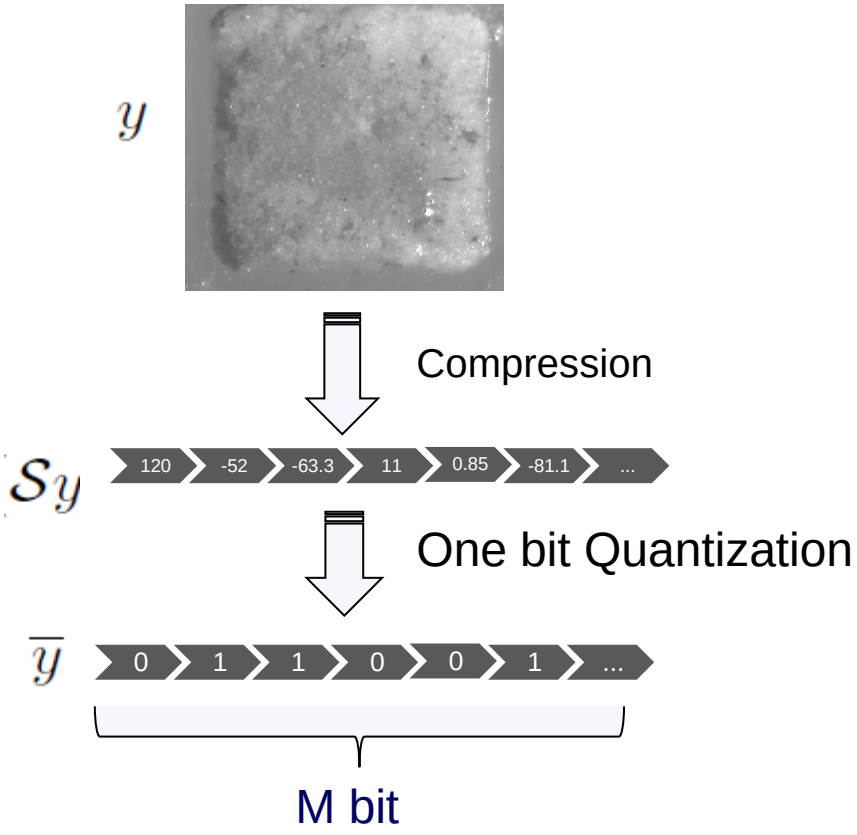


Image Hashing

$$h : \mathbb{R}^N \rightarrow \mathcal{B}^M, \; y \mapsto \overline{y} = H(y) = \mathrm{sign}_{\mathrm{b}}(\mathcal{S}y),$$



Adaptive Image Hashing-Theory

- Let $y = \sum_i \alpha_i \psi_i = \Psi \alpha$ be sparse in a certain basis (Fourier, Wavelet, Gabor, Curvelet),

- By sparse it means that the entries of $\alpha = [\alpha_1, \alpha_2, ..., \alpha_N]$ when sorted from largest to smallest, decay rapidly to zero.

- Adaptive compressing of the signal accounts for a *K*-term approximation, consisting of the terms α with the *K* largest magnitudes.

Non-adaptive Image Hashing--Theory

- A signal that is sparse in one basis can be recovered from $M = O(K \log N/K)$ non-adaptive linear projections onto a basis Φ that is incoherent with the sparsity basis.

- So the signal is approximated by

$$y_M = \Phi y$$

- For instance, random matrices that are incoherent with most known basis functions have most typically used to perform the non-adaptive Compressed Sensing.

Random Binary Hashing

- A random matrix $\Phi = (\Phi_{ij}) \in \mathbb{R}^{M \times N}$ such as Gaussian matrix $\Phi_{ij} \sim_{\text{iid}} \mathcal{N}(0, 1/M)$ is used as the sensing matrix $\mathcal{S}$.

$$\mathbb{P}_{\Phi}\left[\left|\frac{1}{M}\text{dist}_{\text{H}}(\overline{y},\overline{w}) - \text{dist}_{\angle}(y,w)\right| \geq \beta\right] \leq 2\,e^{-2\beta^2 M}.$$

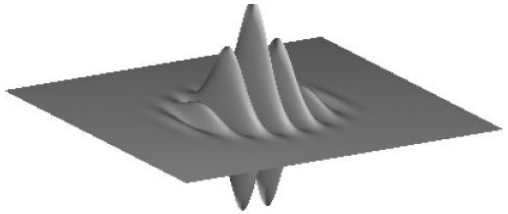
A fast and efficient hashing of the images.

Gabor Binary Hashing

- Sparsity Basis : Gabor
- Gabor Basis : a complete family of localized, oriented, bandpass atoms.

$$g_\psi(t) = \frac{1}{a\sqrt{2\pi}} \sin(\nu \cdot (t-k)) \exp(-\frac{1}{4a^2}\|t-k\|^2),$$

$$\langle g_\psi, y \rangle = \sum_{i=1}^{N} g_{\psi_i} y_i \cong G_\psi^T y,$$



$$\begin{aligned}\Psi(a,\nu_0,\Delta) \;=\; \Big\{&(a,\nu_f,b_m) : \\ &\nu_f = \nu_0(\sin\theta_f, \cos\theta_f),\ \theta_f = 2\pi f/F,\ 0 \le f < F, \\ &k_m = (m_1\Delta, m_2\Delta),\ 0 \le m_i < \lfloor N_i/\Delta \rfloor, i \in \{1,2\}\Big\},\end{aligned}$$

Gabor Binary Hashing

- Let $\psi^{(i)}$ be the parameter vector pointing out the strongest value of Gabor coefficients.

- Sensing matrix is defined:

$$\mathcal{S}_G = [G_{\psi(1)}, G_{\psi(2)}, \ldots, G_{\psi(M)}]^T$$

Experiments -LPUF

- Robustness $\rho_{\mathsf{PFS}} = \Pr[z_r = z_s]$,
  - Database: R=20, Q=60

$$\mathcal{S}_1 = \{y_{rq},\ 1 \leq r \leq R,\ 1 \leq q \leq Q\} \subset \mathbb{R}^N$$

- Physical Unclonabilty

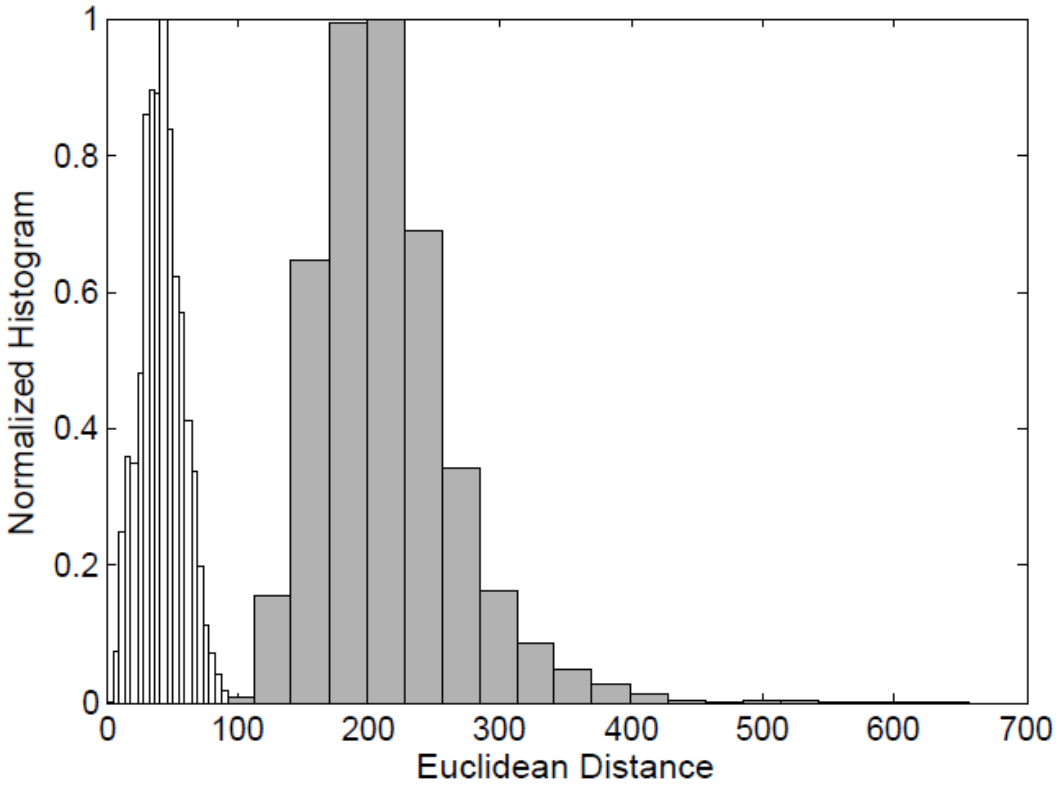
$$PU_{ex\mathsf{PFS}} = \Pr[z_r = z_s : p \neq p'].$$

  - Database: R=1000

$$\mathcal{S}_2 = \{y_r,\ 1 \leq r \leq R\} \subset \mathbb{R}^N$$

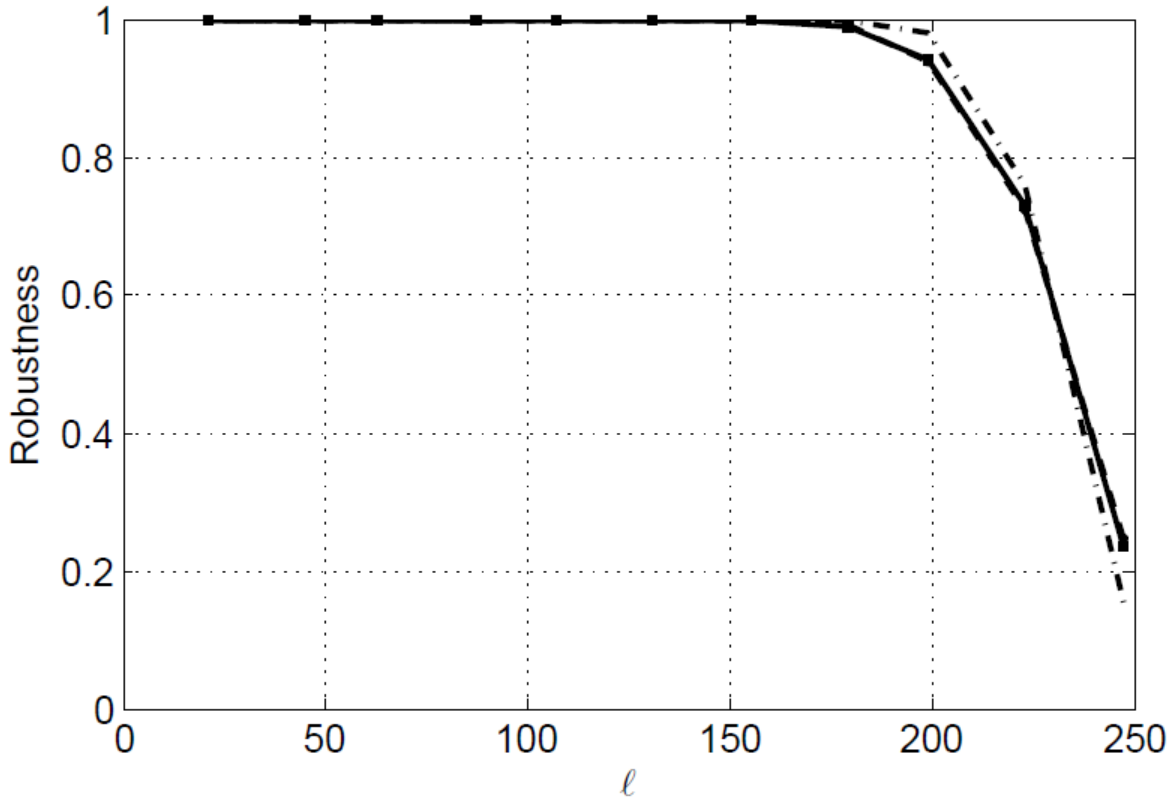
Preliminary analysis of database

Intra and Inter-class Histogram of



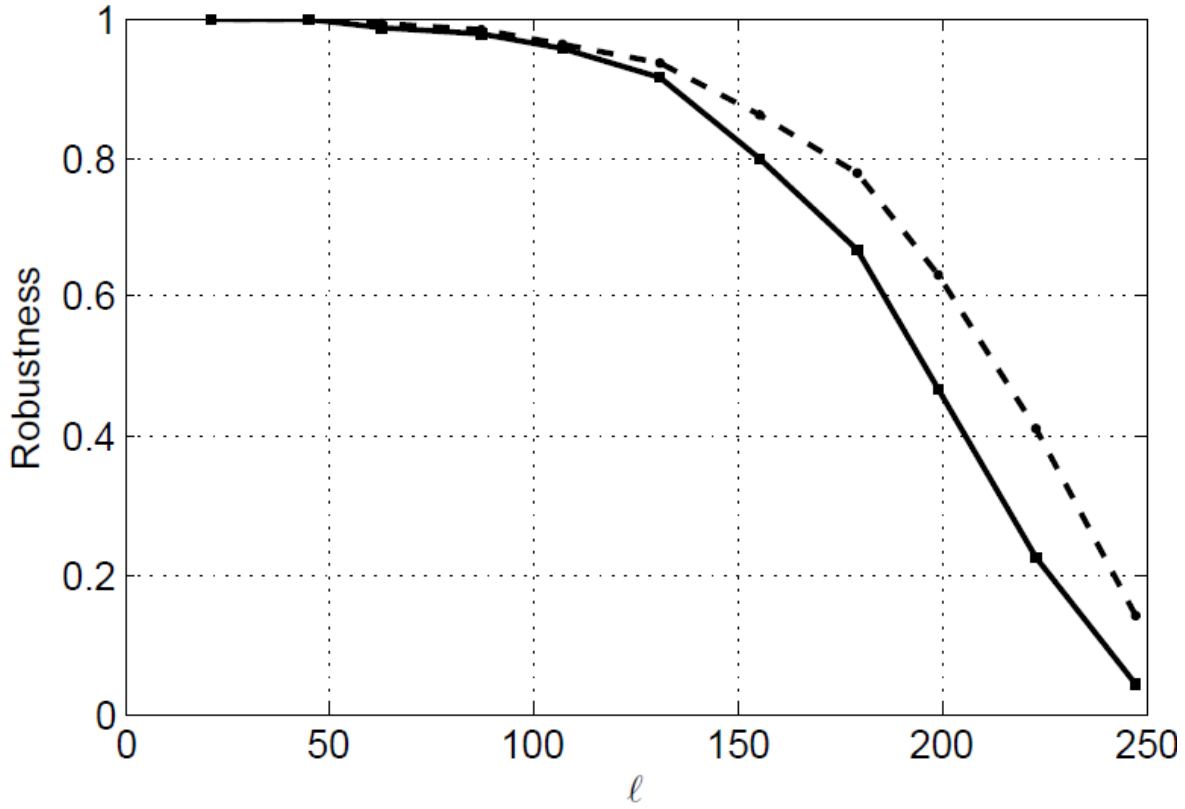
Robustness vs. Length of Identifier

RbEX



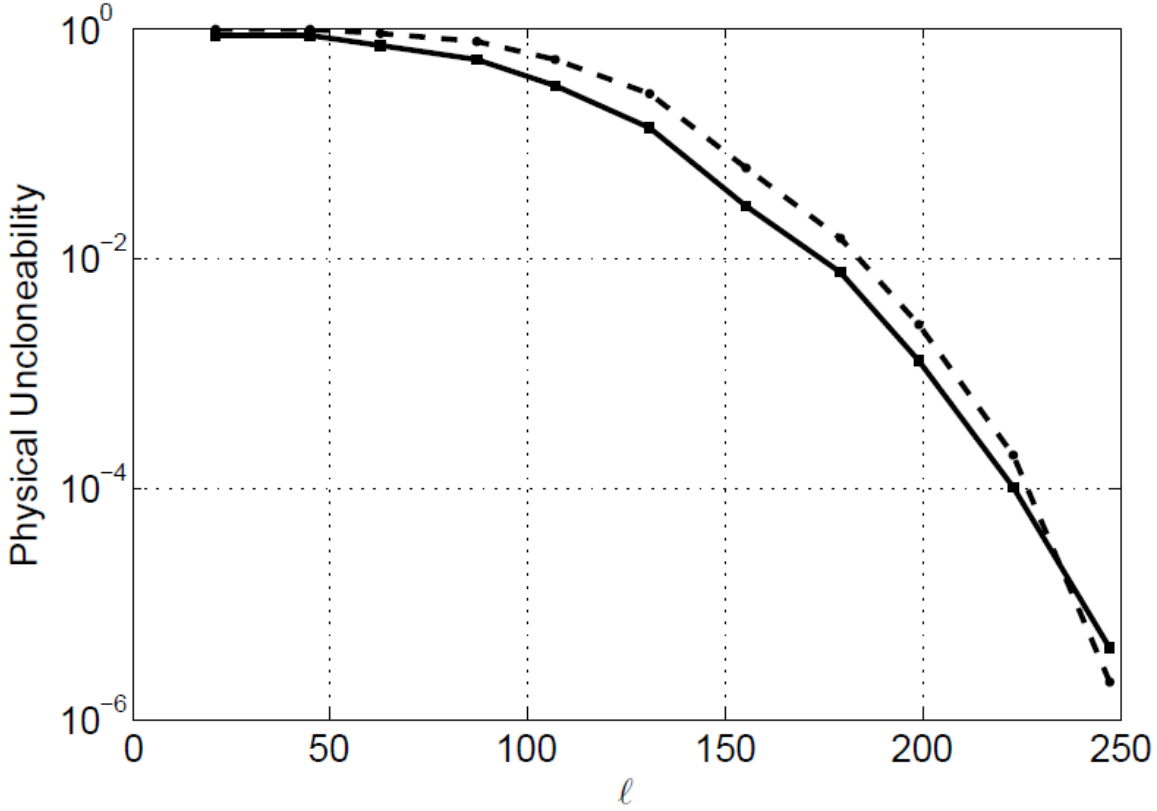
Robustness vs. Length of Identifier

GbEX



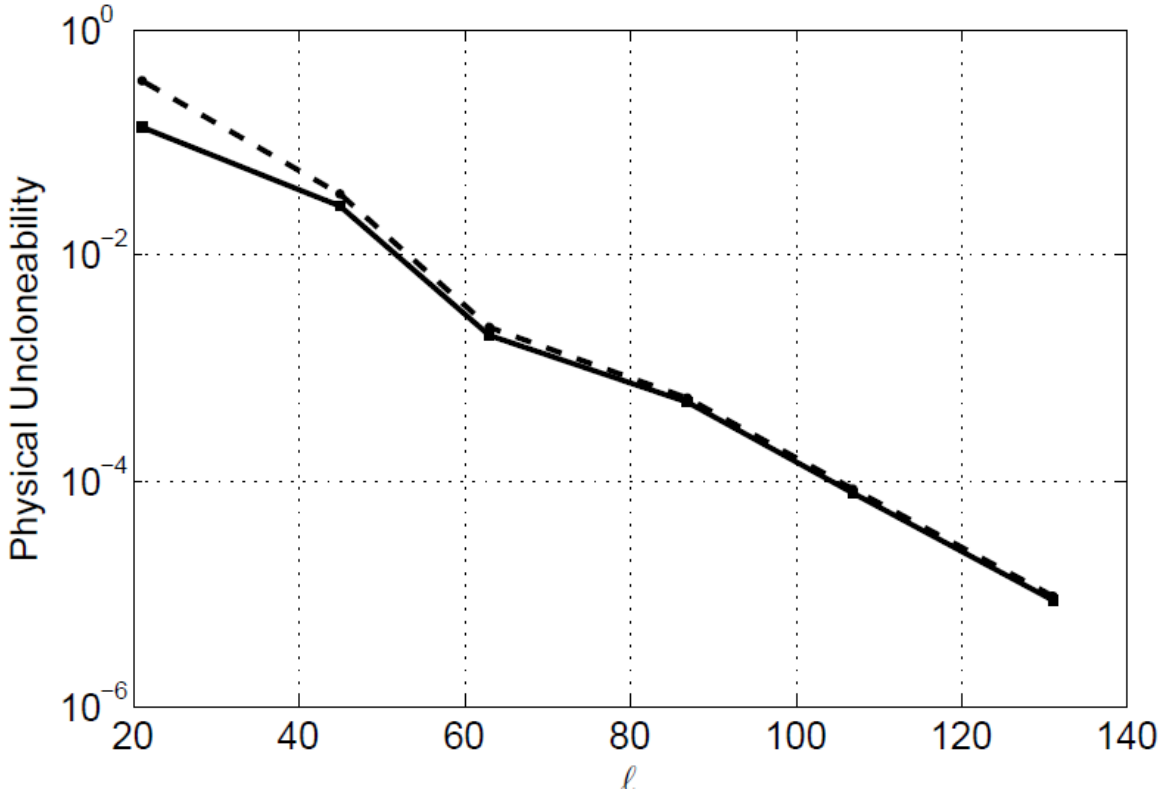
Physical Unclonability vs. Length of Identifier

RbEX



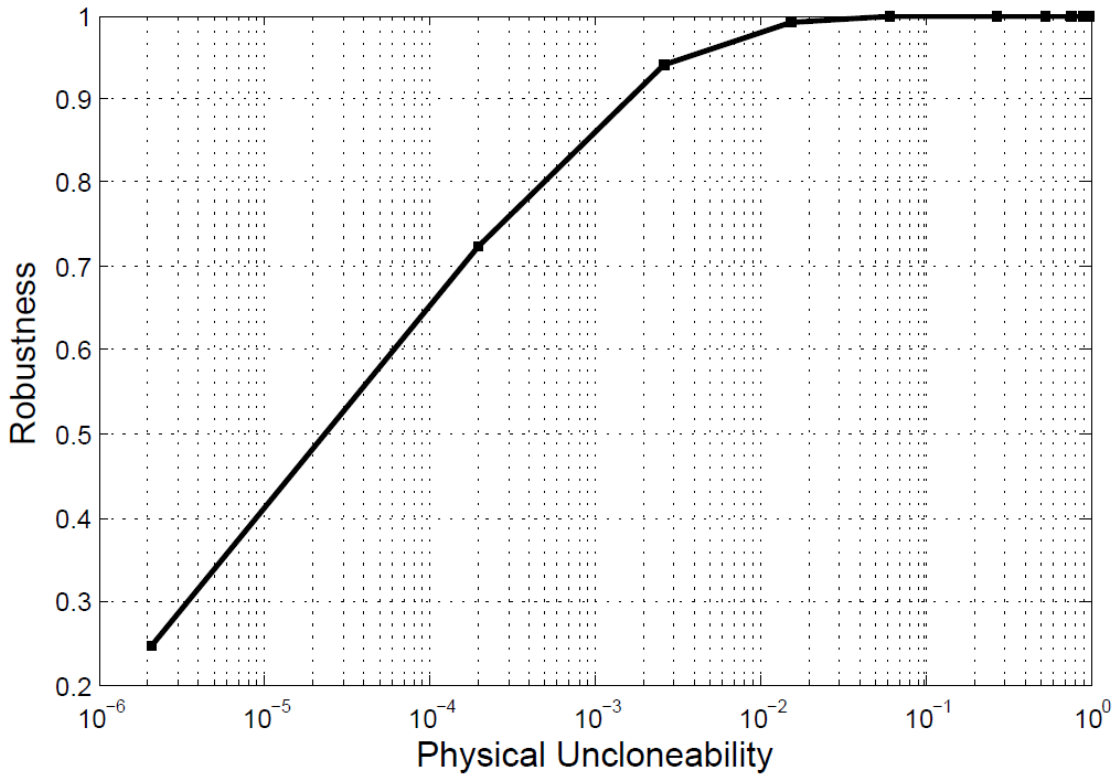
Physical Unclonability vs. Length of Identifier

GbEX



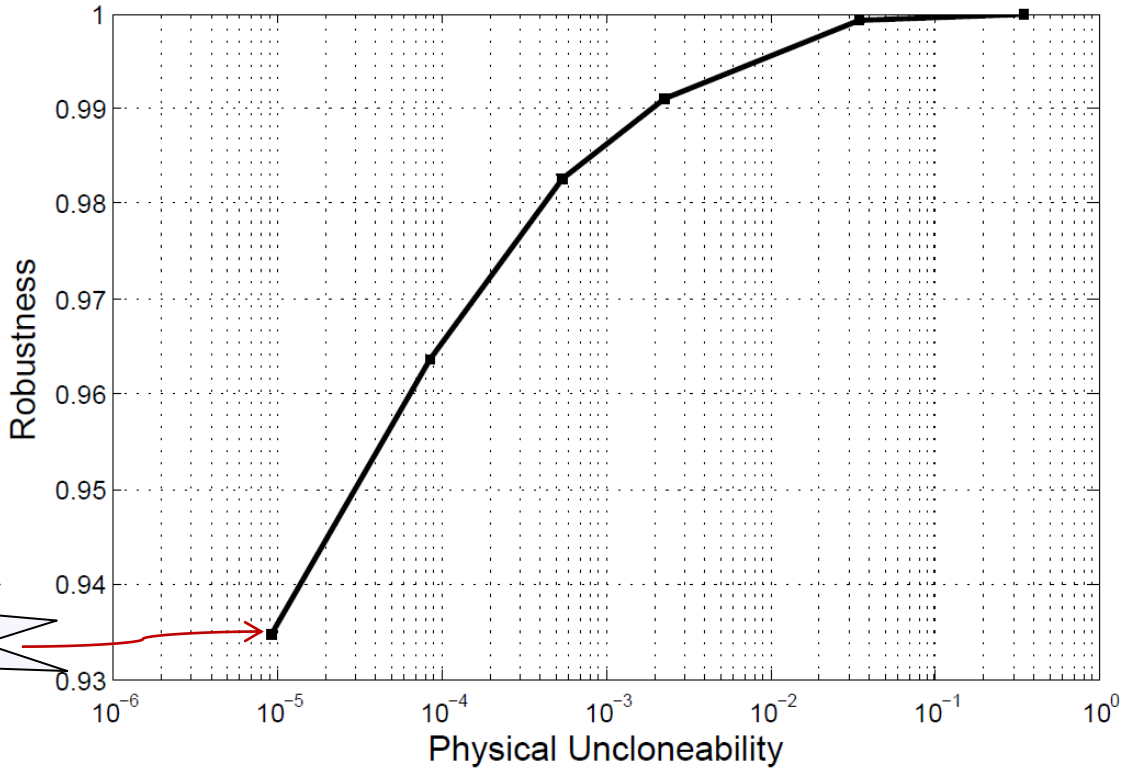
Robustness vs. Physical Unclonability

RbEX



Robustness vs. Physical Unclonability

GbEX



$0.94,10^{-5}$

Thank you