New Insights to Key Derivation for Tamper-Evident Physical Unclonable Functions (PUFs)

Vincent Immler, Karthik Uppund

Conference on Cryptographic Hardware and Embedded Systems, Atlanta, Aug 26, 2019

PUF in a Nutshell: Biometrics of Objects

apply stimulus

random response

PUF Object

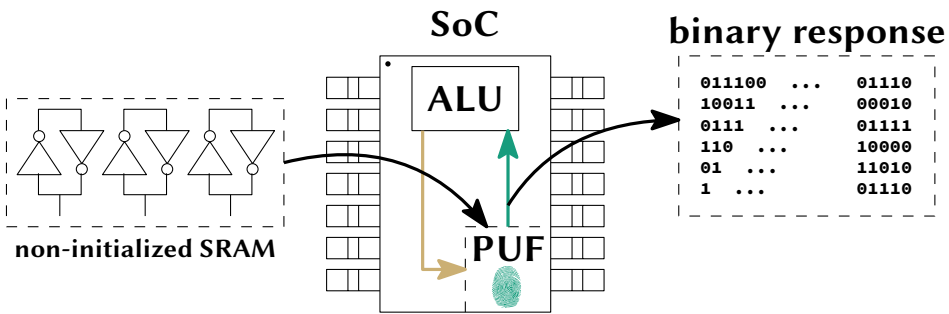
Properties

easy to evaluate

hard to predict

…sounds great! Let's use this in HW crypto!

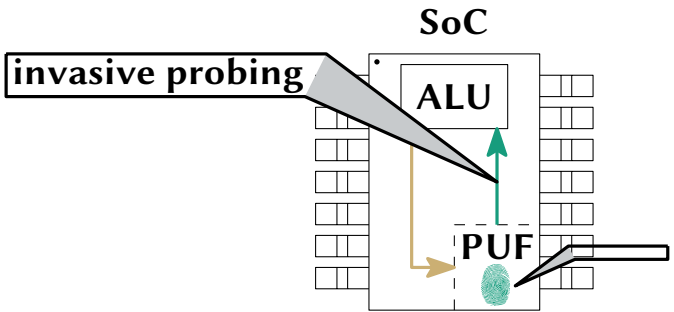
PUF in a Nutshell: Example



key derivation from response instead of key storage!

advantages: delayering and optical analysis cannot reveal key
disadvantages: noisy response necessitates error-correction

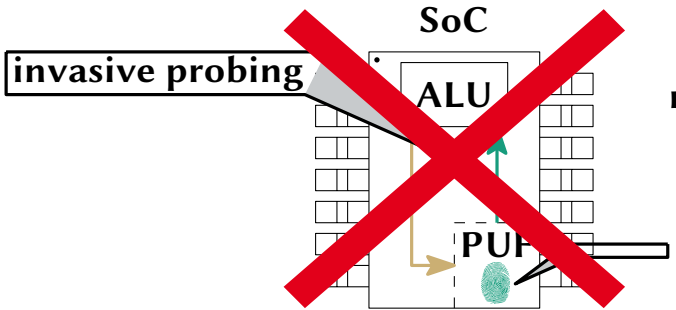
PUFs and Probing (In-)Security



What about other physical attacks?

cf. “On the Physical Security of Physically Unclonable Functions” by Shahin Tajik

PUFs and Probing (In-)Security: A Common Misconception

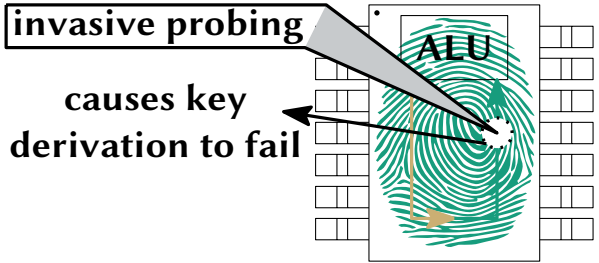


not claimed and
not designed
to resist attack

most PUFs ≠ protection from live physical attacks

(they are not tamper-evident, still needed:active meshes and other countermeasures)

Idea of Tamper-Evident PUFs



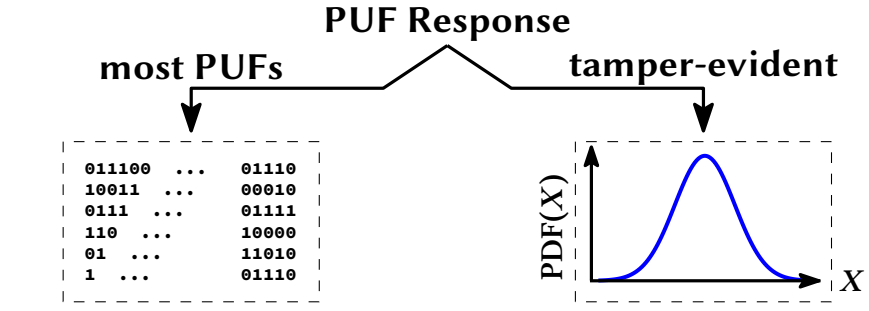
PUF Assumptions

- encloses system
- sensitive to tampering
- self-protective

tamper-evident PUF = protection from probing attacks

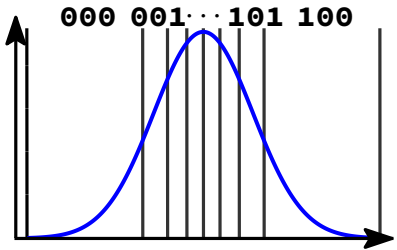
examples: Coating PUF (CHES'06), Waveguide PUF ('15), B-TREPID (HOST'18)

Key Derivation based on Type of PUF



Two Well-Known Quantization Schemes

equiprobable

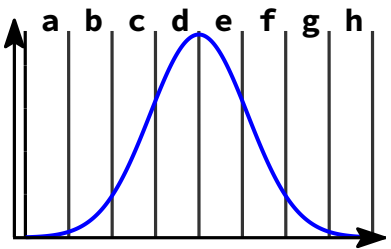


i.i.d. bits ✓

no bias ✓

noise? → binary ECC

equidistant

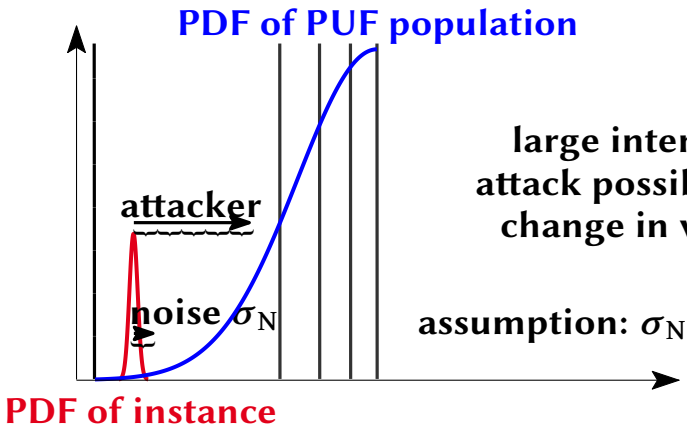


symbols! no (i.i.d) bits!

biased!

noise? → ECC?

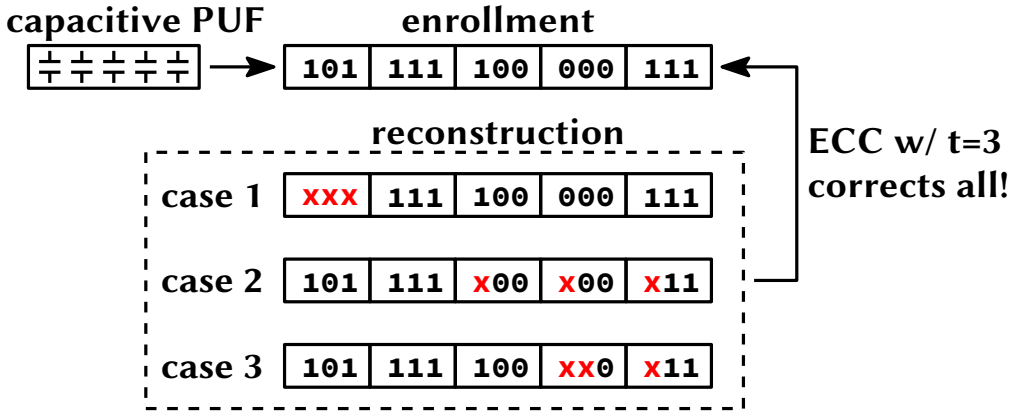
Equiprobable Quantization: Partial Insensitivity to Attacks



large intervals:
attack possible w/o
change in value!

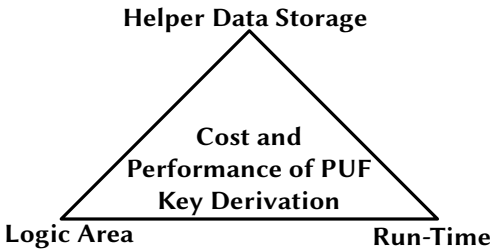
assumption: σ_N < attacker

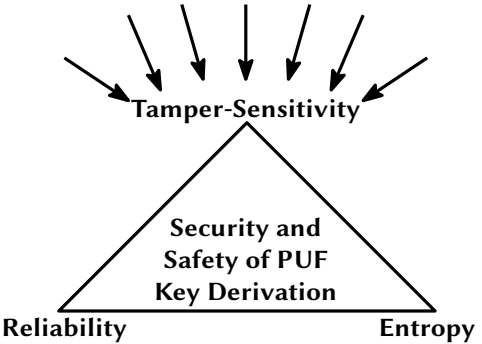
Missing Selectivity of Binary ECC for Respones w/ Multiple Values



(plus: bit string per capacitor < #intervals → large magnitude errors with only t = 1)

Tamper-Sensitivity as High-Level Goal for PUF Key Derivation





previous work: strong focus on making PUFs small and lightweight
different approach needed: make PUFs tamper-evident, large, and secure!

Two Definitions for Fair Comparison of Tamper-Sensitivity

max-TS : Maximum Magnitude Tamper Insensitivity

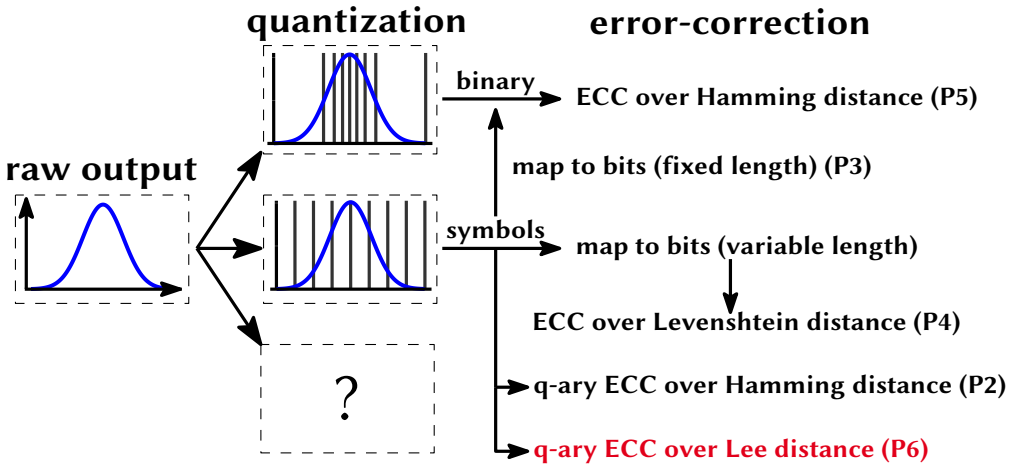
Defines the **maximum magnitude** of the attacker that goes ***undetected*** (worst-case).

min-TS : Minimum Magnitude Tamper Sensitivity

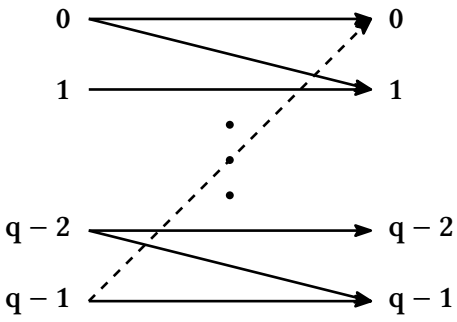
Defines the **minimum magnitude** of the attacker that is ***detected*** (best case).

comparability: express magnitude in multiples of measurement noise σ_{N}
"practically best" physical security for *max*-TS = *min*-TS; and close to 1 (equal to σ_{N})

Zoo of Key Derivation Options for Tamper-Evident PUFs



P6: q-ary Channel Model and Limited Magnitude Codes (LMC)



wrap-around (dashed + thick)
non wrap-around (thick only, use this)

wrap-around (Lee)

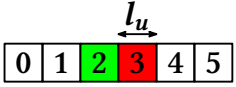
$d_{\text{Lee}}(x, y) = \min((x - y), q - (x - y))$
$d_{\text{Lee}}(0, q - 1) = 1$

non wrap-around (Manhattan)

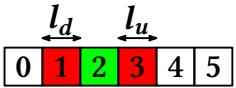
$d_{\text{Lee}}(x, y) = |x - y|$
$d_{\text{Lee}}(0, q - 1) = q - 1$

LMC Types and Result

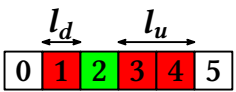
High selectivity of error correction: magnitude, direction, # of magnitude errors



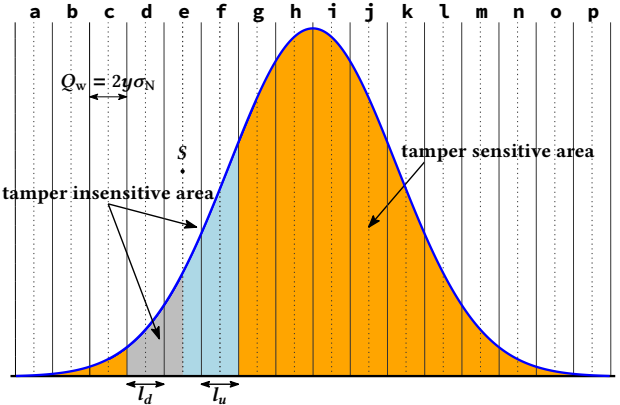
Asymmetric



Symmetric



Bidirectional



Results

Coating PUF parameters (node = single capacitor; device = all capacitors)

Profile	y	L	z	ECC(n, t)	$\mathrm{H}_{\infty}^{\mathrm{eff}}$ [bit]	$\mathrm{TS}_{\mathrm{node}}^{\mathrm{max}}$ [σ_{N}]	$\mathrm{TS}_{\mathrm{device}}^{\mathrm{max}}$ [σ_{N}]	Distance Metric
P1	5.4	8	128	–	267	5.4	692	none
P2	2.3	32	4	RS(31, 7)	122	148	4352	$\mathrm{d}_{\mathrm{H}\mid S}$
P3	3.6	16	5	BCH(127, 2)	265	116	1577	$\mathrm{d}_{\mathrm{H}\mid 2}$
P4	4.95	12	1	VT$(\cdot, 1)$	276	65	693	$\mathrm{d}_{\mathrm{Lev}}$
P5	2.87	8	2	BCH(255, 4)	320	112	2994	$\mathrm{d}_{\mathrm{H}\mid 2}$
P6	2.1	64	1	LMC(63, 10)	319	6.3	395	$\mathrm{d}_{\mathrm{Man}}$

Conclusions and Future Work

- Tamper-evident PUFs are important for highest physical security
- Physical design and key derivation must be optimized for tamper-sensitivity
- Formalized tamper-sensitivity to better assess PUF key derivation
- Proposed new scheme to overcome previous limitations
- Updated definitions of Uniqueness and Reliability for Lee/Manhatten metric
- Responses based on symbols/higher-order alphabet
  - Benefits of same concept when applied to regular PUFs?
  - Impact of same concept on strong PUFs?
- Future work: investigate better quantization options

Contact Information

Vincent Immler

Central Office for Information Technology
in the Security Sector (ZITiS)

For government inquiries only:
vincent.immler@zitis.bund.de

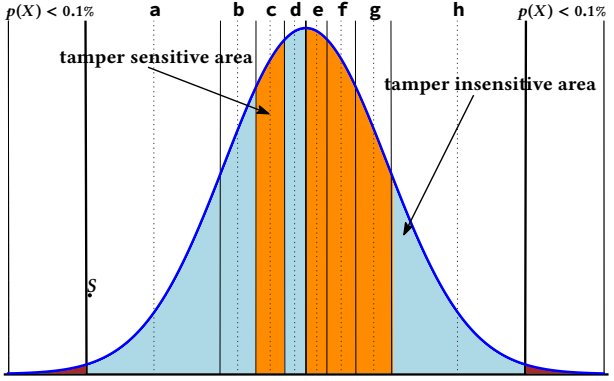
All other inquiries:
science+ches2019@mm.st

This work was performed while with Fraunhofer Institute AISEC.

Thank You!
Questions?

Backup

Profile 5: Equiprobable Quantization + BCH-based Code-Offset



$$\mathrm{TS}^{\max}_{\mathrm{node}} = \sum_{i=1}^{L} \mathrm{width}(Q_i)$$
$$\mathrm{TS}^{\max}_{\mathrm{device}} = z\,t\,\mathrm{TS}^{\max}_{\mathrm{node}} + (v - z\,t) \cdot Q_{\max}/2$$
$$\mathrm{TS}^{\min}_{\mathrm{node}} = 3 \cdot Q_{\min}/2 + \epsilon \qquad \text{iff } t = 1$$
$$\mathrm{TS}^{\min}_{\mathrm{device}} = z\,t\,3 \cdot Q_{\min}/2 + Q_{\min}/2 + \epsilon$$

$\mathrm{grayCode}(0) = 00..0_{\log 2(q)}$
$\mathrm{graycode}(q-1) = 10..0_{\log 2(q)}$