PRACTICAL ASPECTS OF QUANTIZATION AND TAMPER-SENSITIVITY FOR POKS

2016-01-20

Vincent Immler, Maxim Hennig, Ludwig Kürzinger, Georg Sigl

Fraunhofer
AISEC

AGENDA

- Introduction
- Related Work
- Quantization for POKs
- Case Study
- Conclusion

Fraunhofer AISEC

Introduction

- Physical Unclonable Functions (PUFs) based on manufacturing variations
- Variations must be hard to predict and easy to evaluate
- Applications of PUFs in general:
  - Key storage
    - PUFs *not* being tamper-evident, e.g. SRAM-PUF
    - PUFs being tamper-evident, e.g. Coating-PUF ← *focus of this work*
  - Challenge-Response authentication
- Tamper-evident PUFs often named „Physically Obfuscated Key“ (POK)
- Physical attacks (tampering)
  - Drilling, cutting, removal → likely to change POK („tamper-evident“)
  - Probing attempts → improbable to read POK („read-proof“)

Introduction

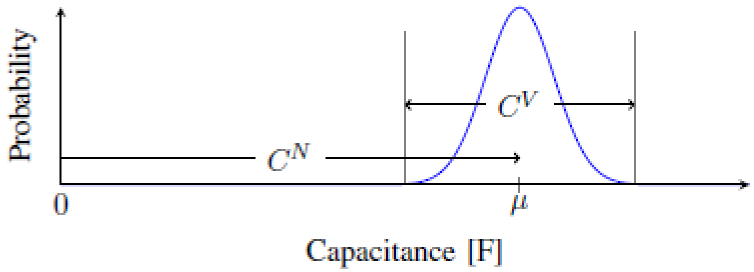
- Certain standards (e.g. FIPS 140-2 Level 4) mandate protection mechanisms to achieve physical security of a certified device
  - Board-level protection, i.e., PCB and its components
  - IC-level protection, i.e., integrated circuit and its package
- Standards require tamper-detection and response mechanism
  - Attacks shall be detected by protected device
  - Response shall protect sensitive data, e.g., by means of zeroization
- POKs as ideal candidate for protected key storage
  - POK as „Key-Encryption-Key“ → other keys of the system and its main software depend on derived key of the POK („tamper-proof“ data)
  - Physical attack destroys POK → encrypted data cannot be recovered

Introduction

- Using a POK requires a process to generate a key
  - Measurement of variation (e.g., analog-to-digital conversion via ADC)
  - Quantization-scheme of raw measurement data ← *focus of this work*
  - Additional post-processing
- From a cryptographic point of view, the generated *key* shall be
  - Unique for each device and uniformly distributed
  - Reliable such that each generation attempt yields the same key
- *Quantization* can be optimized towards
  - Key quality (uniqueness, equi-probability of bits)
  - Reliability (likelihood of obtaining the same key each time)
  - Tamper-sensitivity (sensitivity towards attacks) ← *important!*

Tamper-Sensitivity?

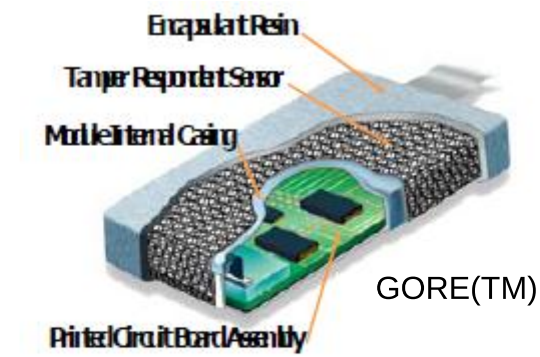
- Example: POK consists of multiple capacitances, each is composed of:
  - Nominal capacitance: C^N
  - Variation due to manufacturing: C^V (relevant for POK values)
- What is the smallest shift (caused by an attack) for a single capacitance that goes undetected?
  - Different compared to noise / can it be distinguished from noise?
  - Magnitude of detectable shift depends on resolution of measurement circuit, present noise, and post-processing (i.e., quantization, and ECC)

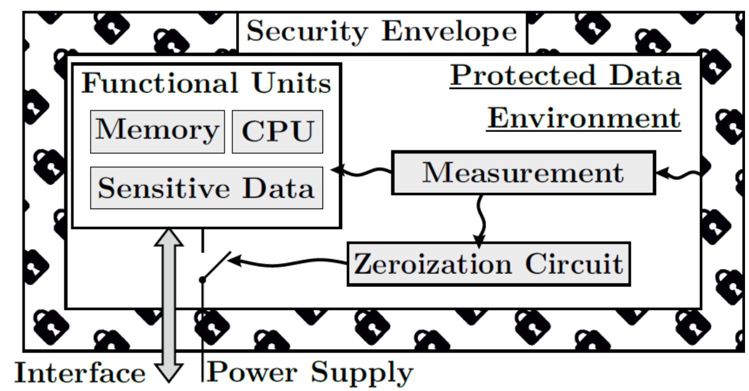


RELATED WORK

What We Do

- Prior work: Devices protected with printed mesh on a flexible substrate
  - Mesh is continuously monitored to detect penetration attempts
  - Monitoring initialized at factory-site and *battery-backed* (active throughout lifetime of device)
- Our work: Use flexible substrate with electrodes as a POK
  - Does *not* require battery
  - *Key generation* to decrypt software of the device / determine integrity
  - Attack=physical destruction of key





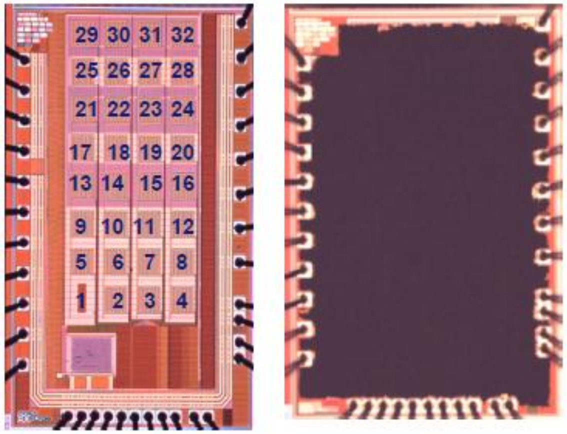
Fraunhofer AISEC

Related Work

- Key generation for PUFs/POKs typically divided in two stages:
  - Key enrollment: key is derived for the first time, *helper data* is generated to support later key reconstruction
  - Key reconstruction: subsequent use of system results in *noisy* values which can be stabilized using the helper data
- Helper data may cause information leakage, i.e., leaks information about the actual key being derived. Leakage shall be negligible!
- Related work primarily considers the binary output of PUFs, e.g. SRAM
  - Corresponding helper data related to Error-Correcting Code (ECC)
  - Many schemes available to choose from
  - Good results for key quality and reliability
  - Due to type of considered PUFs: no tamper-sensitivity

Related Work

- Alternatives needed for the noisy m-bit (integer value) output of a POK
  - Pre-processing techniques to transform data (e.g., DCT)
  - Quantization
- Coating PUF (CHES 2006, Tuyls et. al.)
  - Random dielectric particles cover top of IC
  - Capacitive sensors measure capacitance
  - Key generation:
    - Measurement of capacitance
    - Equi-probable quantization of data
    - Additional Error-Correcting Code (ECC)

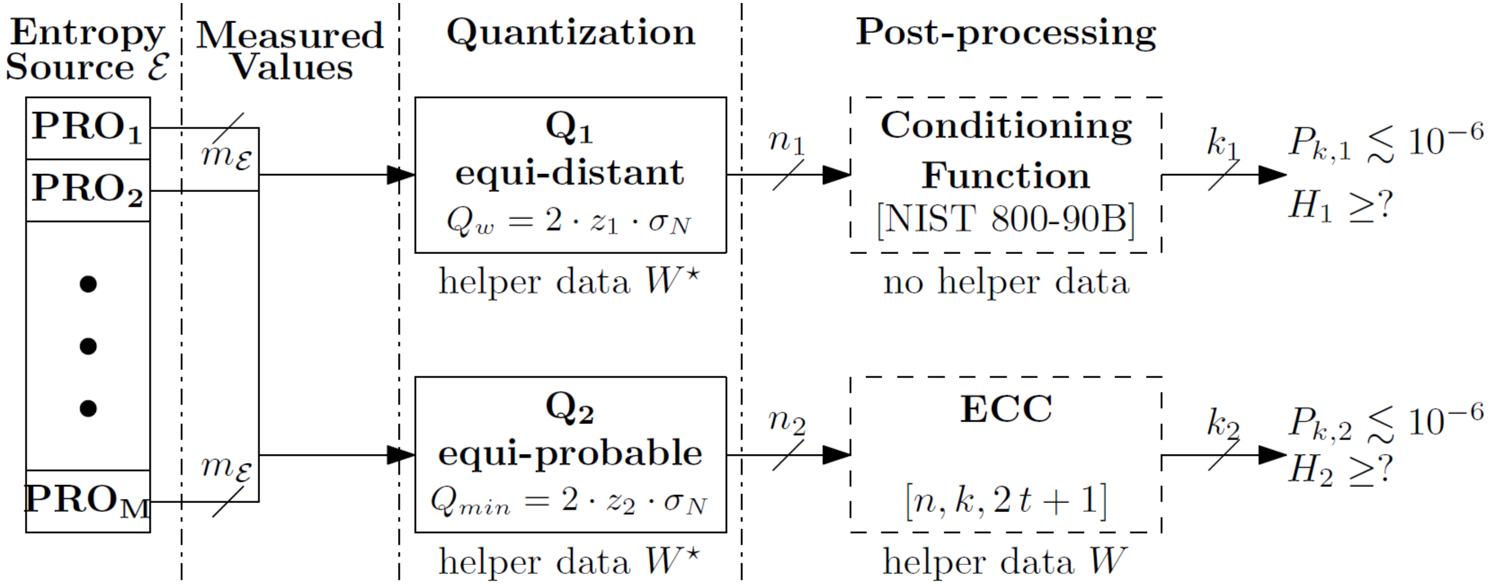


Fraunhofer AISEC

QUANTIZATION FOR POKS

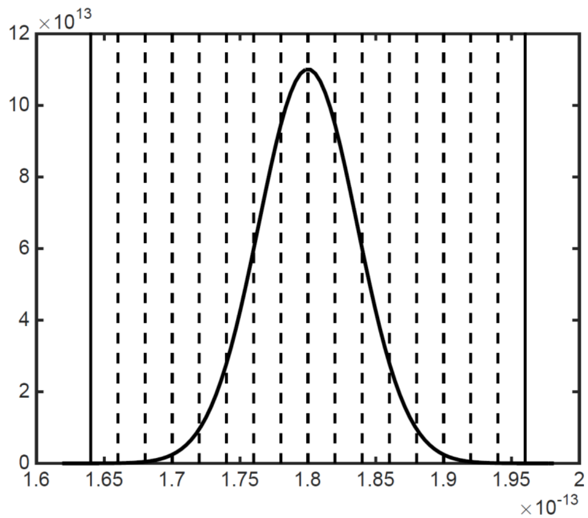
Quantization for POKs

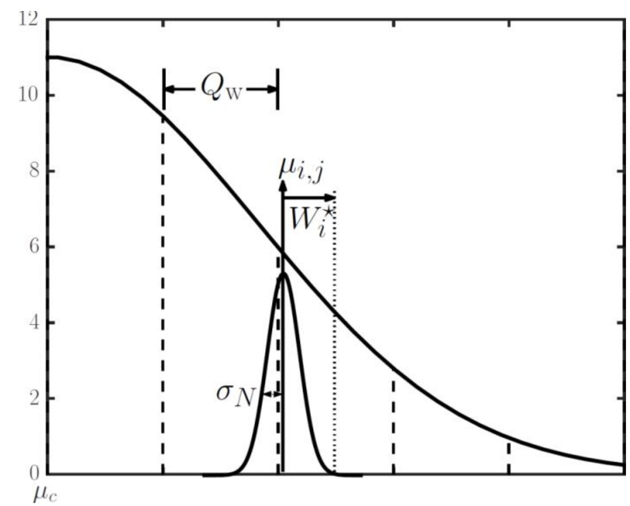
- Analysis based on comparison of two different quantization strategies
  - Equi-distant quantization yields intervals with same width (Q1)
  - Equi-probable quantization yields equi-probable bits (Q2)
- Post-processing steps vary accordingly



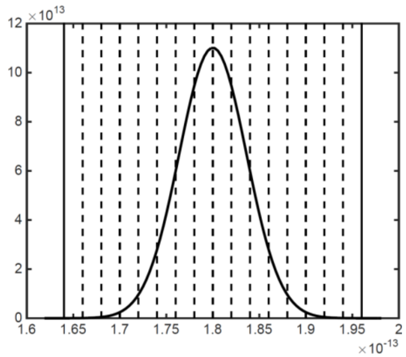
Equi-Distant Quantization

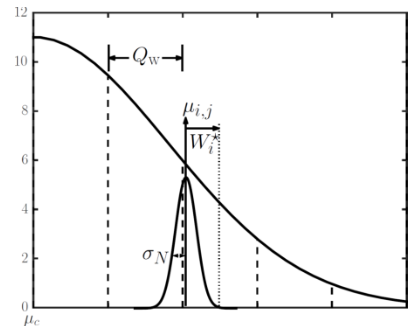
- Enrollment: Divide range of values in evenly spaced intervals
  - Measure POK-values multiple times and average to “remove” noise
  - Determine interval width and compute offset to middle of interval
- Reconstruction:
  - Measure POK-value once, apply offset and quantization





Equi-Distant Quantization

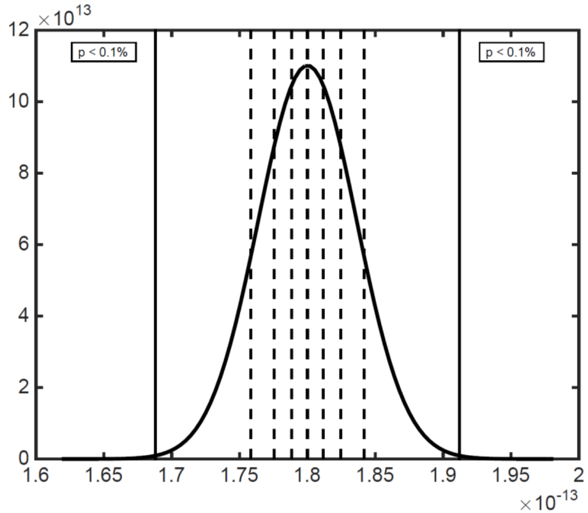


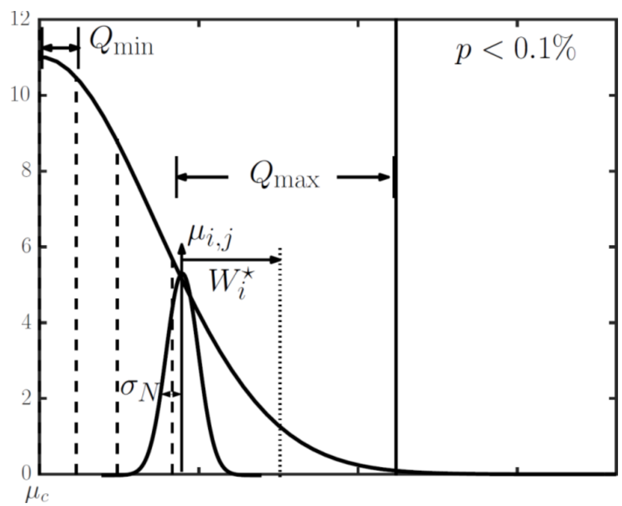


- Reliability:
  - Based on confidence interval $\mathrm{CI} = [-z\sigma_N, z\sigma_N]$
  - Noise level must be determined (depends on device/application)
- Key quality:
  - Shannon entropy H(F) depends on PDF and number of intervals L
  - Higher number of L causes H(F) to approach the differential entropy
  - Resulting bits of quantization *not* equi-probable (requires hash)
- Considering possible attacks
  - I(F,W*): No information can be extracted
  - Tamper-sensitivity: Maximum shift for each interval is the same
- Limitations of this approach: Difficult to apply ECC

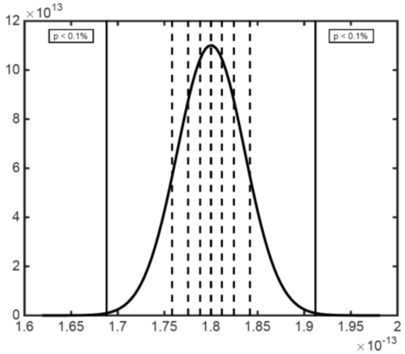
Equi-Probable Quantization

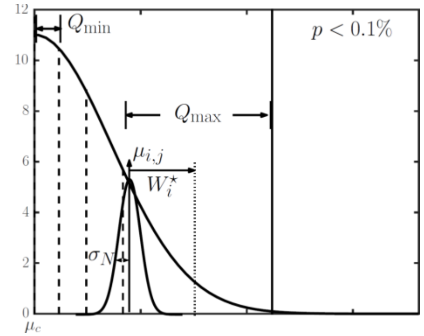
- Enrollment: Divide range of values in equi-probable intervals
  - Measure POK-values multiple times and average to “remove” noise
  - Determine interval width and compute offset to middle of interval
- Reconstruction:
  - Measure POK-value once, apply offset and do quantization





Equi-Probable Quantization



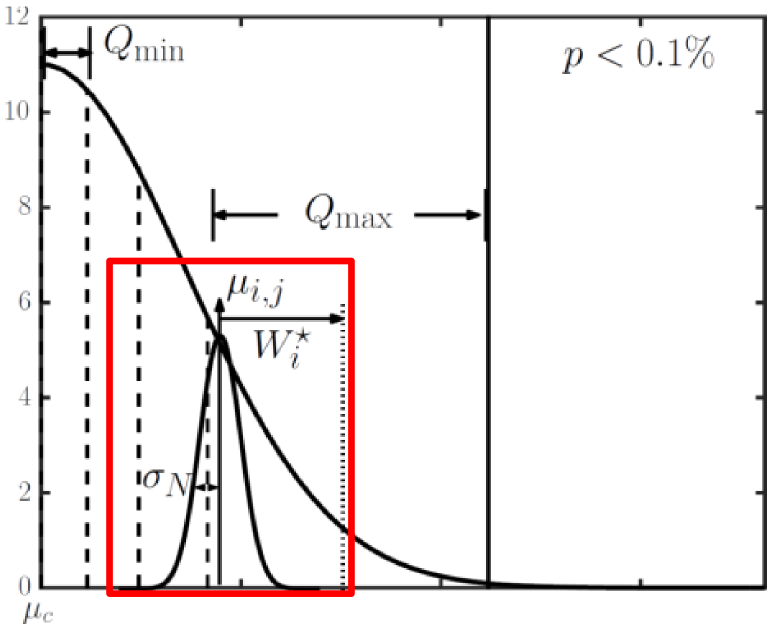


- Reliability:
  - Based on confidence interval of smallest interval
  - Noise level must be determined (depends on device/application)
- Key quality:
  - Shannon entropy H(F) solely depends on number of intervals L
  - Resulting bits are already equi-probable
- Considering possible attacks
  - see next slides
- Limitations
  - see next slides

Fraunhofer AISEC

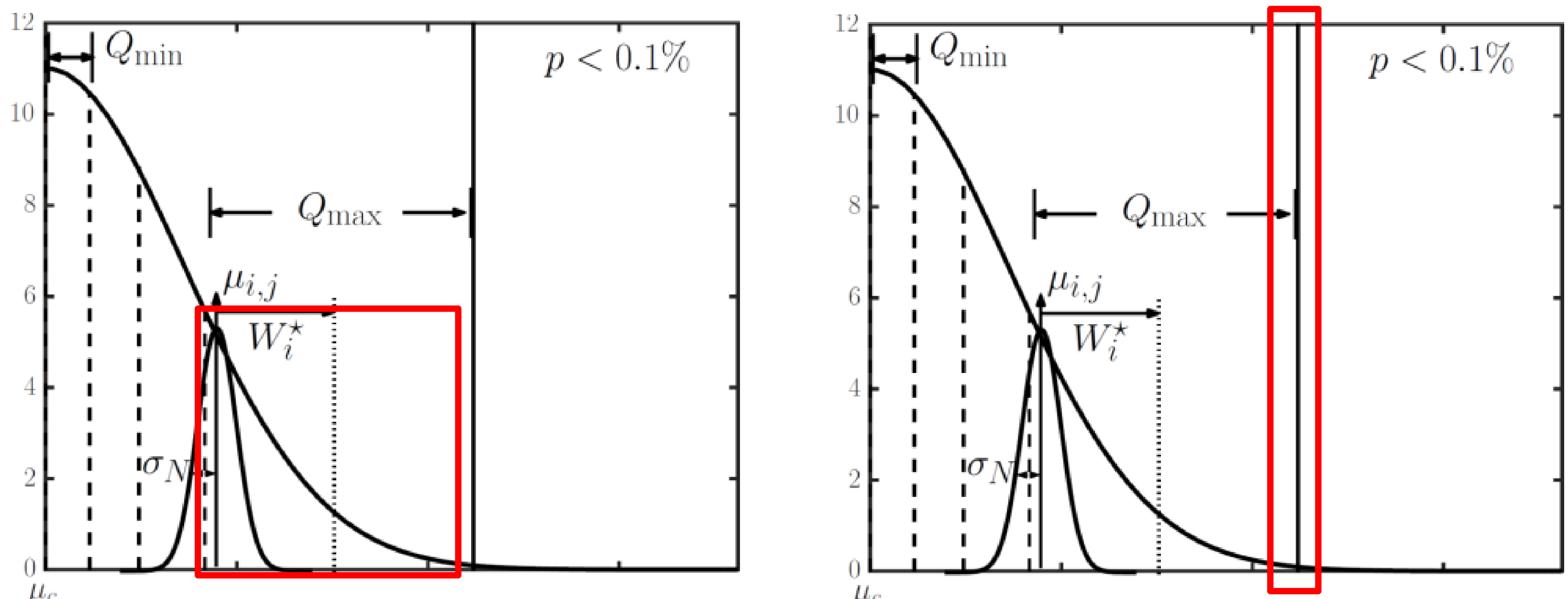
Equi-Probable Quantization: Weakness #1

- Observation:
  - Smallest interval: Q_min
  - Largest interval: Q_max
  - Offset W* can exceed Q_min/2
- → I(F,W*) leaks information about F
- → depending on value of W*, helper data of quantization may fully determine quantized value of F
- *even worse:* for outermost interval, this value has highest probability to occur due to underlying PDF



Equi-Probable Quantization: Weakness #2

- Outermost intervals are less tamper-sensitive than innermost intervals
- Option 1: Valid range is limited by measurement range (bad)
- Option 2: Valid range is limited by boundary “guard” (better)



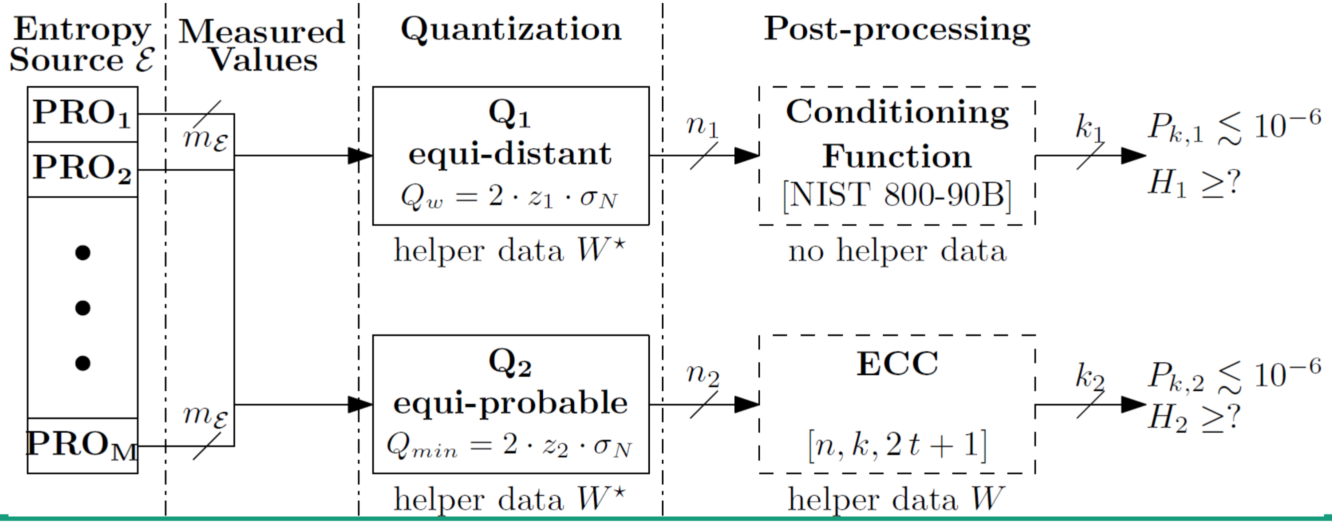
Fraunhofer AISEC

Can these Weaknesses be Mitigated?

- Weakness: information leakage
  - One could limit range of W* to 0.5*Q_min
  - Leakage is reduced but W* is still biased
  - At the same time: maximum shift attacker can do increases
- Weakness: tamper-sensitivity
  - Outermost interval can be made smaller with guard / increases rejects
  - Still, outermost intervals will be less sensitive to attacks

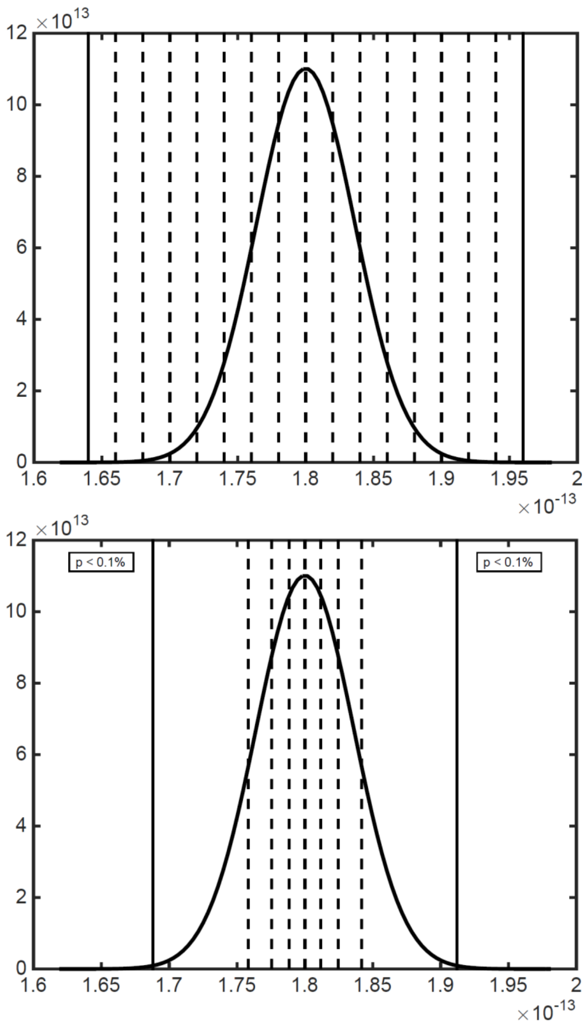
Considered Parameters for the Key Generation

- Key mismatch probability, should be less than 10^(-6)
- I(F,W*) should be negligible
- Shannon entropy H(F)
- Worst-case shift by attacker not being detected (tamper-sensitivity)
- n bit (total number of bits extracted)
- k bit (key bits after all processing steps)



Fraunhofer AISEC

Analysis Results: Quantization Profiles (P1,P2,P3,P4)



$\mathbf{P}_1$, Q_2: Same approach as for the coating PUF in [10].

$\mathbf{P}_2$, Q_2: Modifed approach of [10] to limit $Q_{\max}$.

$\mathbf{P}_3$, Q_2: The leakage of the helper data $W^\star$ is reduced.

$\mathbf{P}_4$, Q_1: The proposed equi-distant quantization.

Parameter	$\mathbf{P}_1$	$\mathbf{P}_2$	$\mathbf{P}_3$	$\mathbf{P}_4$
Quantizer	Q_2	Q_2	Q_2	Q_1
$P_k \lesssim 10^{-6}$	yes	yes	yes	yes
$\mathrm{I}(F, W^\star)$	leakage	leakage	reduced	negligible
$\mathrm{H}(F)$ in bit	3	3	3	~ 2.9
$Q_{\min}$ $[2\,\sigma_N]$	2.9	2.9	2.9	5.3
$Q_{\max}$ $[2\,\sigma_N]$	inf	17.5	17.5	5.3
W^A_{worst} $[\sigma_N]$	inf	17.5	29.2	5.3
n bits	90	90	90	120
k bits [a]	66.4	66.4	66.4	60
t bits [b]	4	4	4	–

[a] For Q_2, k is based on an optimal error correcting code [10], e.g., a code with parameters $[n, k, 2\,t+1]$. For Q_1, k is half the size of n due to requirements stated in NIST 800-90b.
[b] t bits an error correcting code corrects. Considered as negative impact on tamper-sensitivity.

Fraunhofer AISEC

Implications

- Equi-probable quantization offers best worst-case sensitivity among all considered variants
- Equi-probable quantization should only be used if information leakage is reduced and boundary guard is used (P3)
- Side note: By using ECC one additionally corrects t bit

Parameter	P_1	P_2	P_3	P_4
Quantizer	Q_2	Q_2	Q_2	Q_1
$P_k \lesssim 10^{-6}$	yes	yes	yes	yes
$I(F, W^\star)$	leakage	leakage	reduced	negligible
$H(F)$ in bit	3	3	3	~ 2.9
$Q_{\min}$ $[2\,\sigma_N]$	2.9	2.9	2.9	5.3
$Q_{\max}$ $[2\,\sigma_N]$	inf	17.5	17.5	5.3
W^A_{worst} $[\sigma_N]$	inf	17.5	29.2	5.3
n bits	90	90	90	120
k bits [a]	66.4	66.4	66.4	60
t bits [b]	4	4	4	–

[a] For Q_2, k is based on an optimal error correcting code [10], e.g., a code with parameters $[n, k, 2\,t+1]$. For Q_1, k is half the size of n due to requirements stated in NIST 800-90b.
[b] t bits an error correcting code corrects. Considered as negative impact on tamper-sensitivity.

Fraunhofer AISEC

Conclusion

- Quantization is an important security aspect for POKs
- Any helper data should be considered for design (W and W*)
- Tamper-sensitivity related to reliability...
  - ... but should be considered a metric on its own
  - ... not necessarily the same as influence by noise
- At stage of quantization:
  - Achieving equi-probability of bits difficult without major drawbacks
  - Additional processing required

Thank you very much for your attention!

Questions?