

# Hardware Intrinsic Security from D Flip-flops



intrinsic ID

TRUST 2010 - Workshop Security Hardware

Geert-Jan Schrijen, Helena Handschuh,  
Pim Tuyls, and Vincent van der Leest

Tuesday, June 22, 2010





# Table of Contents

- Introduction
- PUF framework
- Assessment of D Flip-flop PUF properties
  - Reliability
  - Randomness
- Processing
  - Von Neumann Extractor
  - XOR-ing
- Assessment of data set after processing
- Conclusions

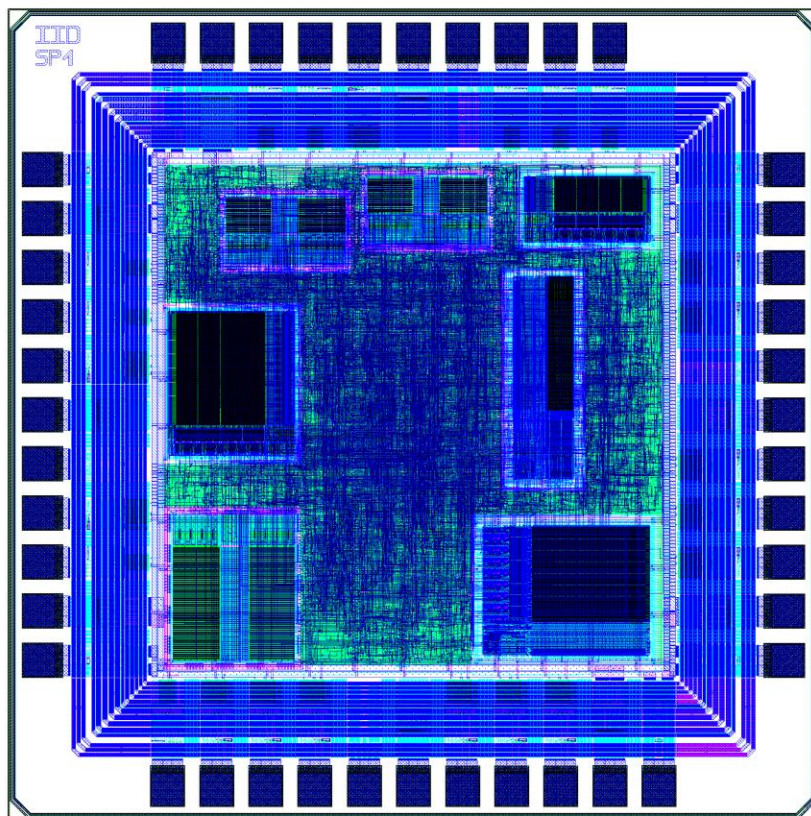


# Introduction

- PUF: Physically Uncloneable Function
- “Fingerprint” based on hardware intrinsic properties that vary due to manufacturing process variations
- DFF PUF is based on start-up pattern of DFF’s
- Comparison with SRAM: DFF can be distributed
- Evaluation properties:
  - Reliability: when PUF responses are measured, the reference measurement should be recognized which was taken at enrollment
  - Randomness: PUF responses of a specific device are random and unpredictable, even given all PUF responses of other devices



# Introduction



All results in this presentation from:  
40 UMC 130nm devices

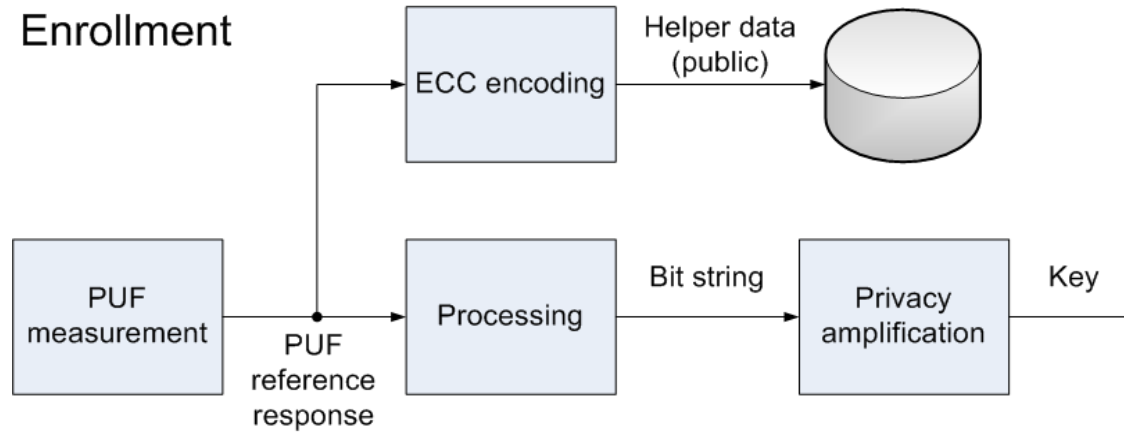
Design shows locations  
of SRAMs very clearly

DFF can not be seen  
1024 distributed DFFs

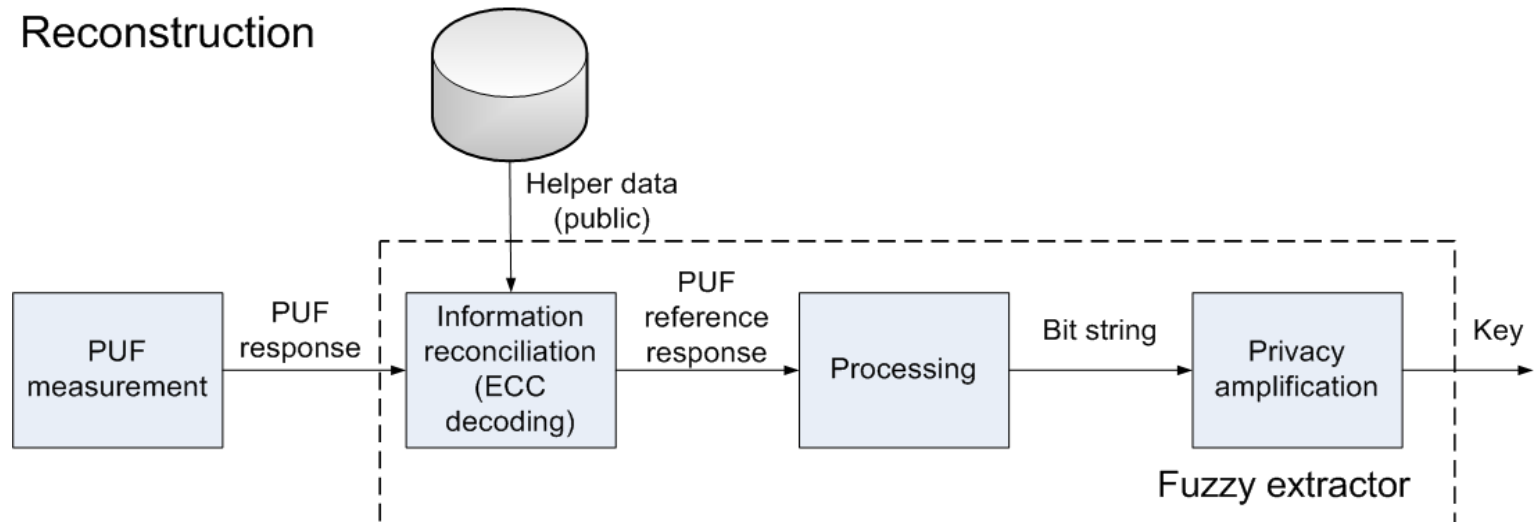


# PUF framework

## Enrollment



## Reconstruction





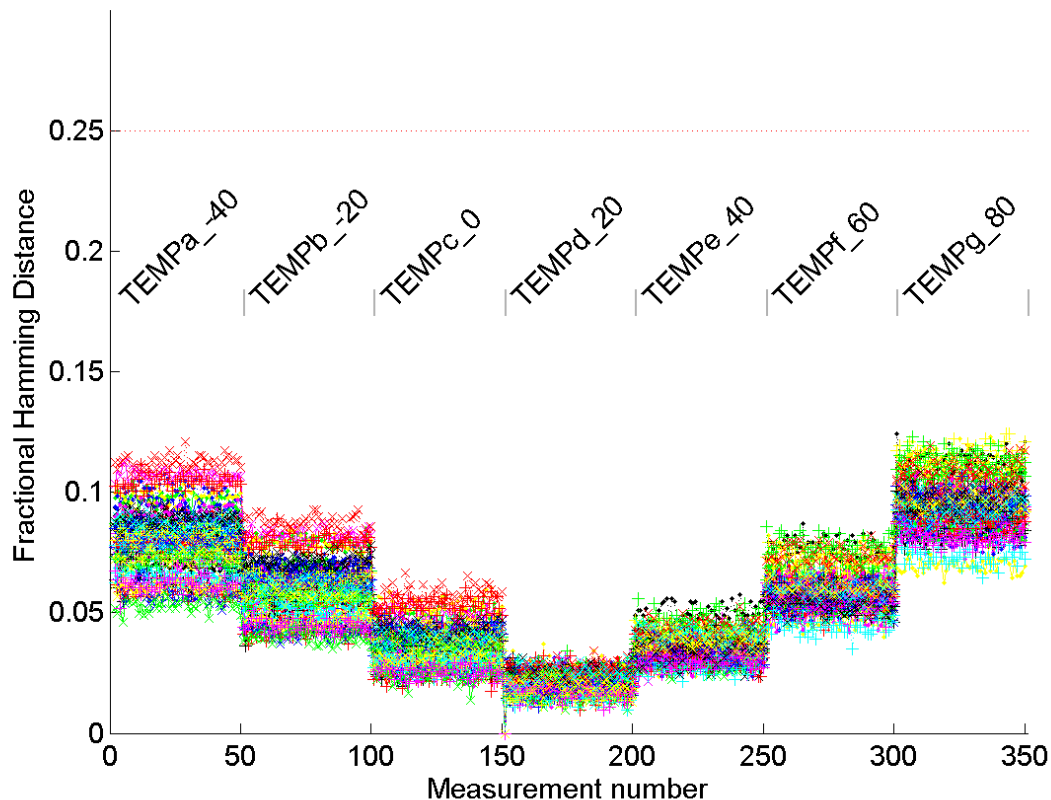
# Assessment of D Flip-flop PUF properties

- Reliability has been assessed using
  - Temperature test
  - Ageing test
- Randomness has been assessed using:
  - Hamming Weight Test
  - Inter-class Uniqueness Test
  - CTW Compression Test
  - NIST Randomness Tests



# Assessment of Reliability PUF response

Within-class fractional hamming distances



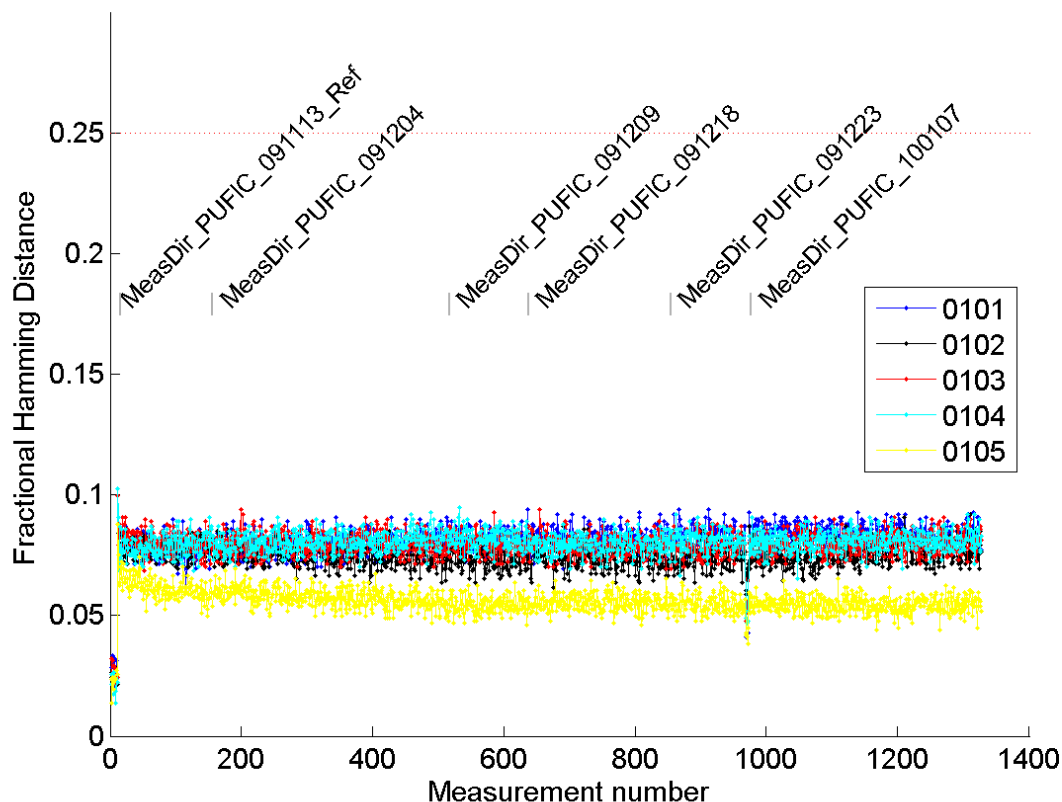
## Temperature Test:

HD is always below 13% for temperatures from  $-40^{\circ}\text{C}$  to  $+80^{\circ}\text{C}$



# Assessment of Reliability PUF response

Within-class fractional hamming distances



## Ageing Test:

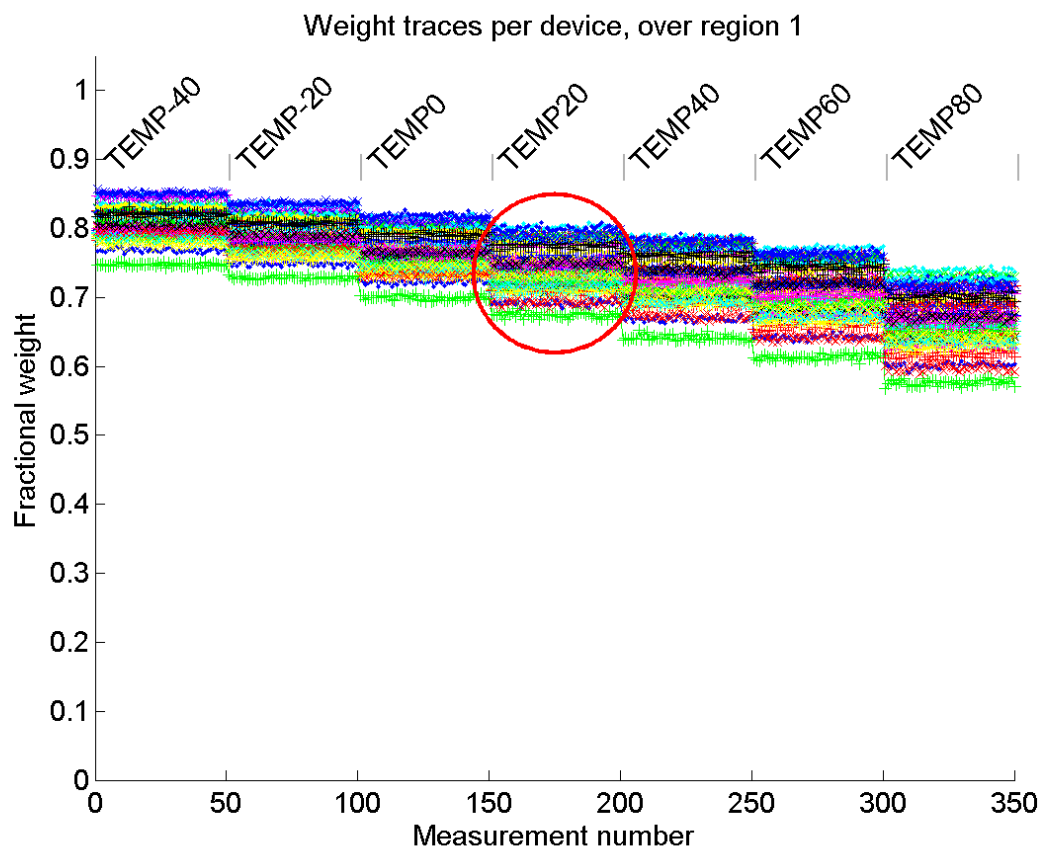
8 weeks at +80°C and 1.1\*Vdd

HD is not increasing

HD is always below 10%



# Assessment of Randomness PUF response



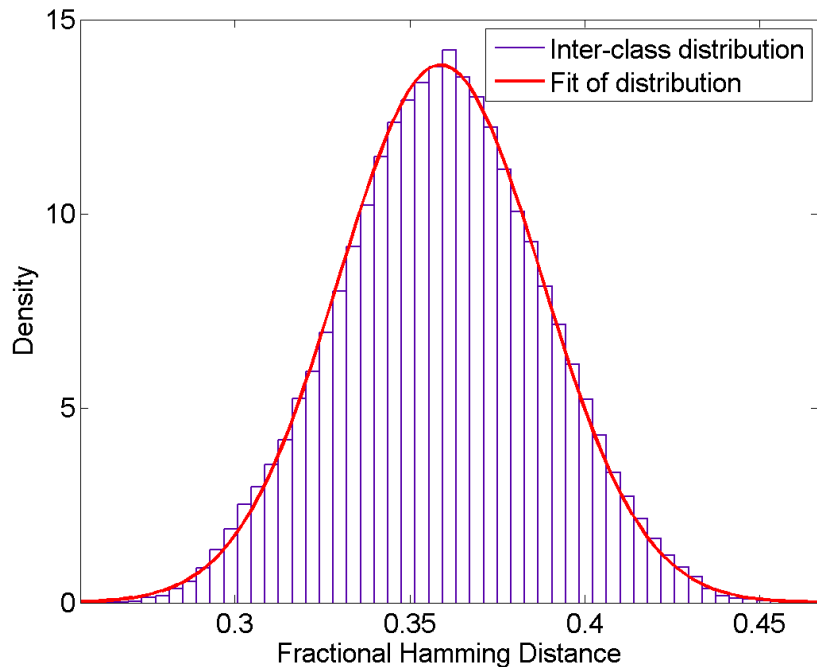
## Hamming Weight:

HW during enrollment is  
between 0.68 and 0.84

HW is much higher than 0.5



# Assessment of Randomness PUF response



## Inter-class Uniqueness:

Distribution approximated as

Gaussian with  $\mu=0.36$  and  $\sigma=0.029$

Positive: inter-class HD always  $> 0.26$

Negative: not centered around 0.5

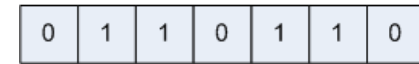
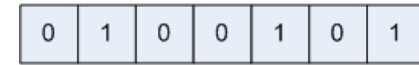
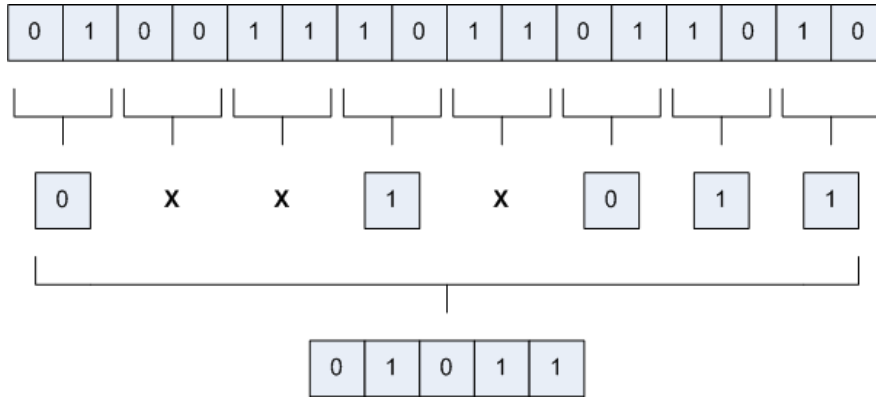
Data	Input length	Output length	Compress ratio
DFF data	40960	33282	81.3%

## CTW Test:

Since compress ratio  $< 100\%$  it is possible to compress data using CTW algorithm



# Processing



Data set	Von Neumann	XOR	String length
1VNM3XOR	1	3	69
0VNM4XOR	0	4	256
0VNM5XOR	0	5	204
0VNM6XOR	0	6	170

Four data sets are tested with frequency and serial test to determine which will be evaluated on randomness



# Processing

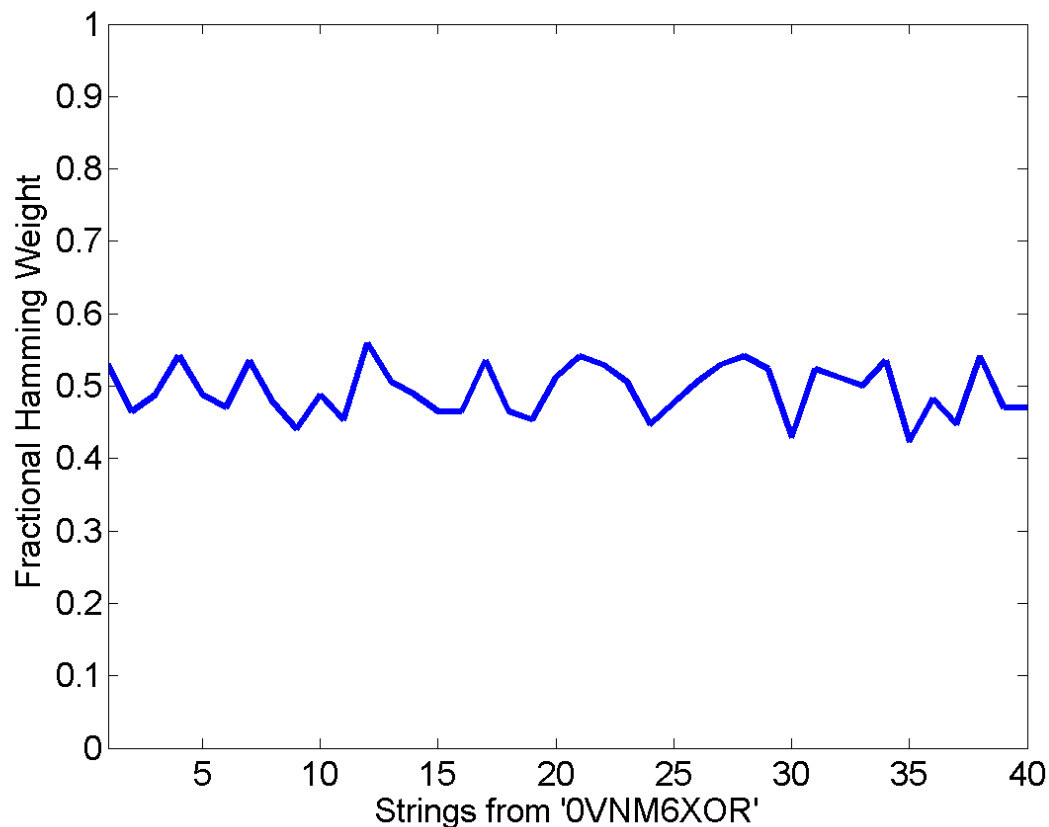
Frequency test	$\alpha = 0.1$	$\alpha = 0.05$	$\alpha = 0.01$
1VNM3XOR	5	5	2
0VNM4XOR	7	4	3
0VNM5XOR	5	4	1
0VNM6XOR	2	1	0

Serial test	$\alpha = 0.1$	$\alpha = 0.05$	$\alpha = 0.01$
1VNM3XOR	5	3	2
0VNM4XOR	9	7	2
0VNM5XOR	5	4	2
0VNM6XOR	1	0	0

Based on these results  
“0VNM6XOR” has been  
selected to evaluate further



# Assessment Randomness after processing



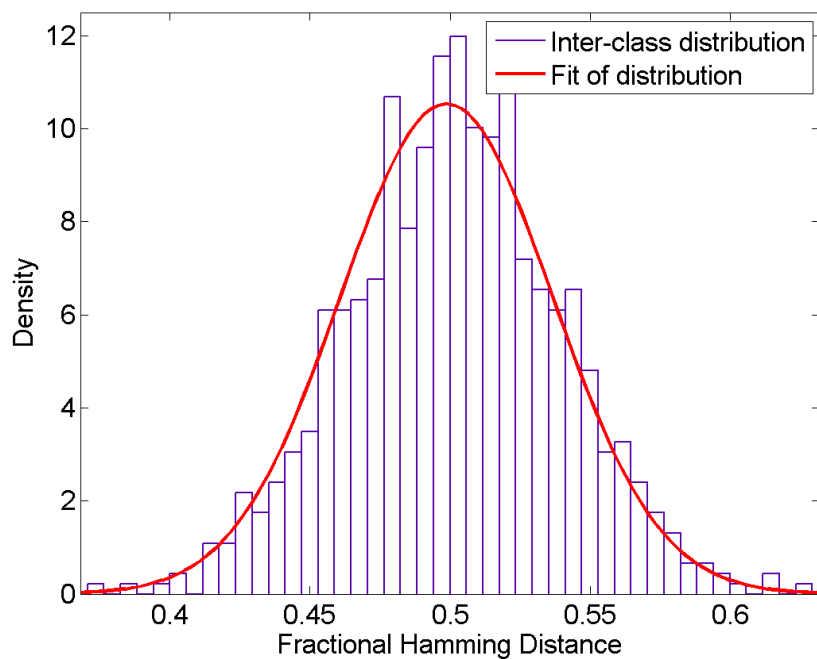
## Hamming Weight:

HW after processing is  
between 0.45 and 0.55

HW is centered around 0.5



# Assessment Randomness after processing



## Inter-class Uniqueness:

Distribution approximated as

Gaussian with  $\mu=0.50$  and  $\sigma=0.038$

Positive: inter-class HD always  $> 0.35$

Positive: centered around 0.5

Data	Input length	Output length	Compress ratio
0VNM6XOR	6800	6807	100%

## CTW Test:

Since compress ratio = 100% it is not possible to compress data using CTW algorithm



# Assessment Randomness after processing

$$p' = p \pm 3 \sqrt{\frac{p(1-p)}{n}} = 0.99 \pm 3 \sqrt{\frac{0.99 \cdot 0.01}{40}} \geq 0.9428$$

## NIST Tests:

$$p' \geq 0.9428 \quad \cap \quad P\text{-value} \geq 0.0001$$

NIST test	$p'$	P-value	Pass/Fail
Frequency test	1.000	0.0571	Pass
Frequency test within block	1.000	0.5341	Pass
Runs test	0.975	0.0909	Pass
Longest runs within block	1.000	0.2430	Pass
Serial test	1.000	0.0151	Pass
Approximate entropy test	1.000	0.2430	Pass
Cumulative sums test	1.000	0.0487	Pass

“0VNM6XOR”  
passes all NIST  
randomness tests  
that are possible for  
this string length



# Conclusions

- D flip-flops contain sufficient randomness in their start-up behavior to qualify as strong, randomly distributed but reliable PUFs
- Using processing it is possible to remove the bias that is present in start-up values of D flip-flops
- Reliability of D flip-flop PUFs over a large range of different temperatures and that static ageing does not degrade the PUF responses have been shown



# Making counterfeiting a thing of the past



[www.intrinsic-id.com](http://www.intrinsic-id.com)