INTRINSIC ID

Secure your digital life™

Hardware Intrinsic Security, from theory to practice

Vincent van der Leest

Intrinsic-ID, Eindhoven, The Netherlands

vincent.van.der.leest@intrinsic-id.com

Table of Contents

Introduction

PUF = Function embodied in a physical structure that consists of many random characteristics originating from uncontrollable process variations during manufacturing

In other words: "Fingerprint" based on hardware intrinsic properties that vary due to manufacturing process variations

Should be:

- Easy to evaluate / measure
- Inseparably bound to the object
- Not reproducible by manufacturer

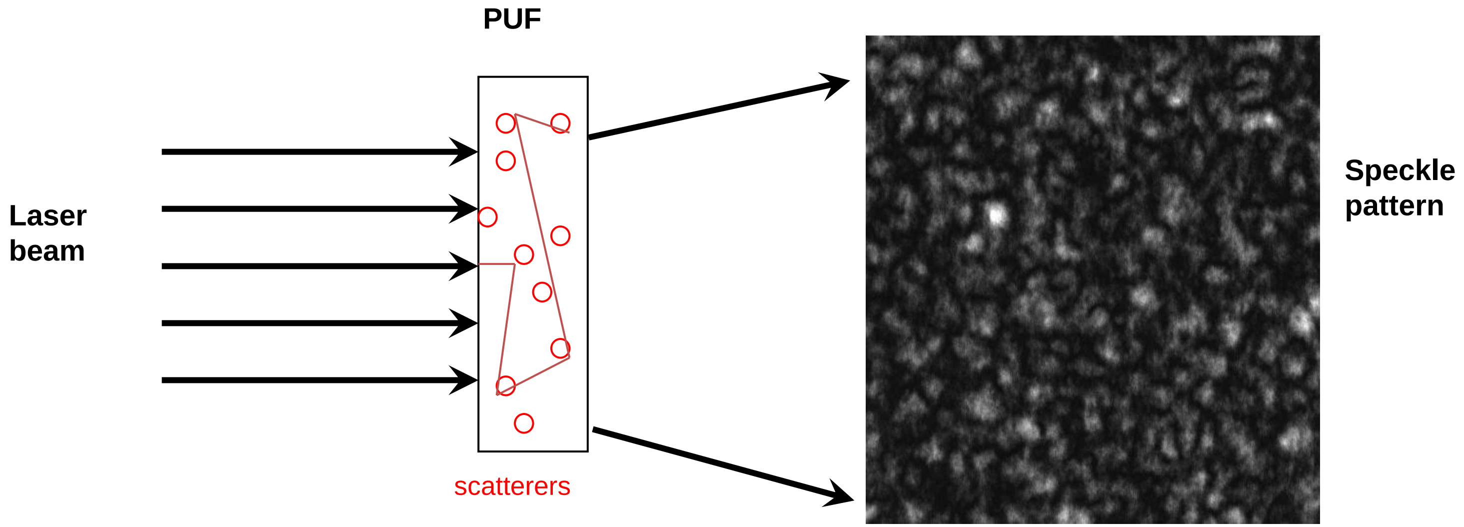
Introduction

Timeline

- …… : Preliminary work on PUF-like technologies
- 2001: First publication of PUFs by Pappu
- 2001: Start of PUF research Philips Research
- 2002: Introduction of silicon based PUFs
- 2006: PUF technology promising enough for Philips to start "business unit"
- 2008: Successful spin-out Intrinsic-ID from Philips

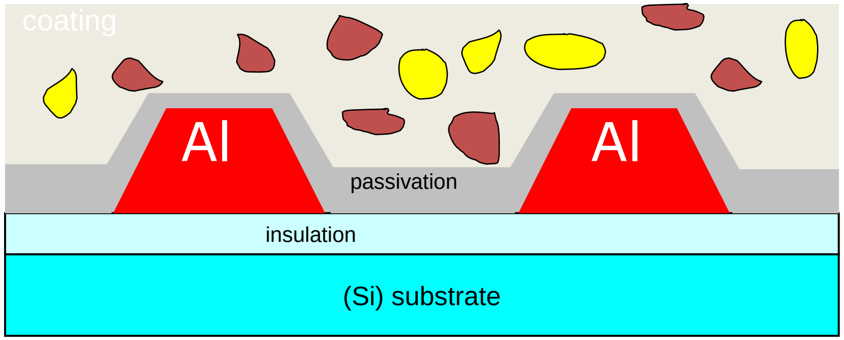
Table of Contents

Optical PUF



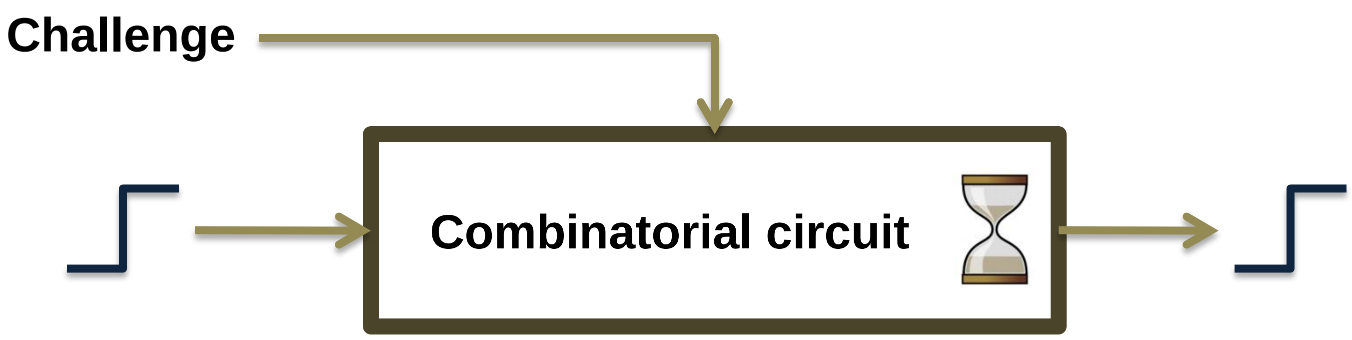
Pro's	Con's
Huge set of C/R-pairs	Difficult to integrate in IC

Coating PUF



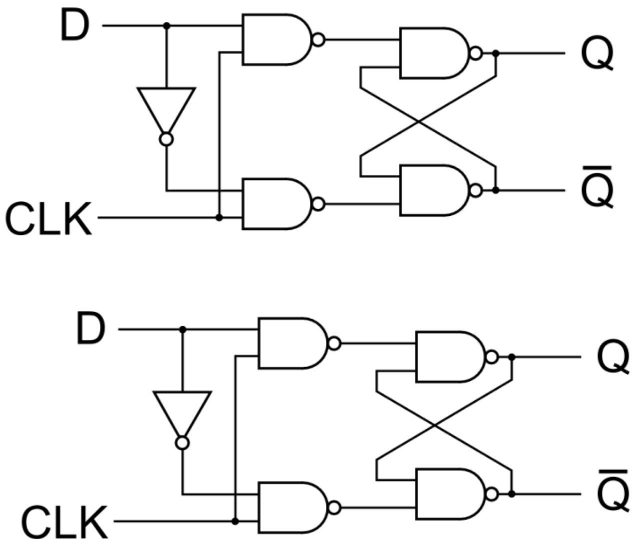
Pro's	Con's
Part of IC	Expensive to produce
	Limited set of C/R-pairs

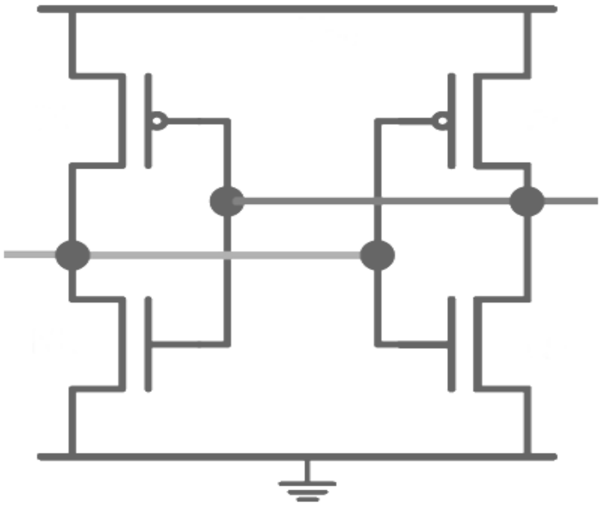
Delay based PUFs



Pro's	Con's
Part of IC	Place and Route constraints due to non-standard components
Relatively large set of C/R-pairs	Susceptible to modeling attacks

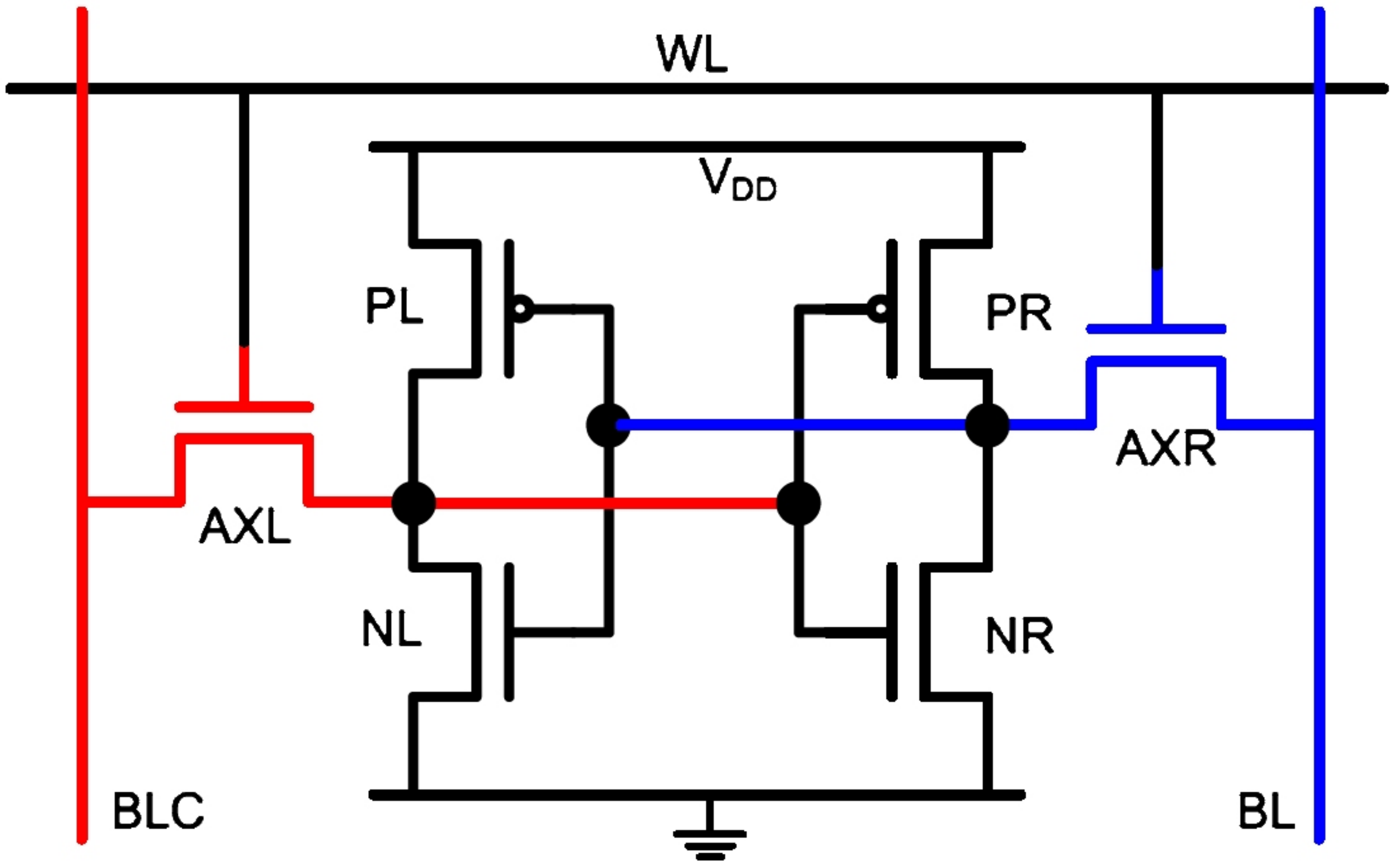
Memory based PUFs



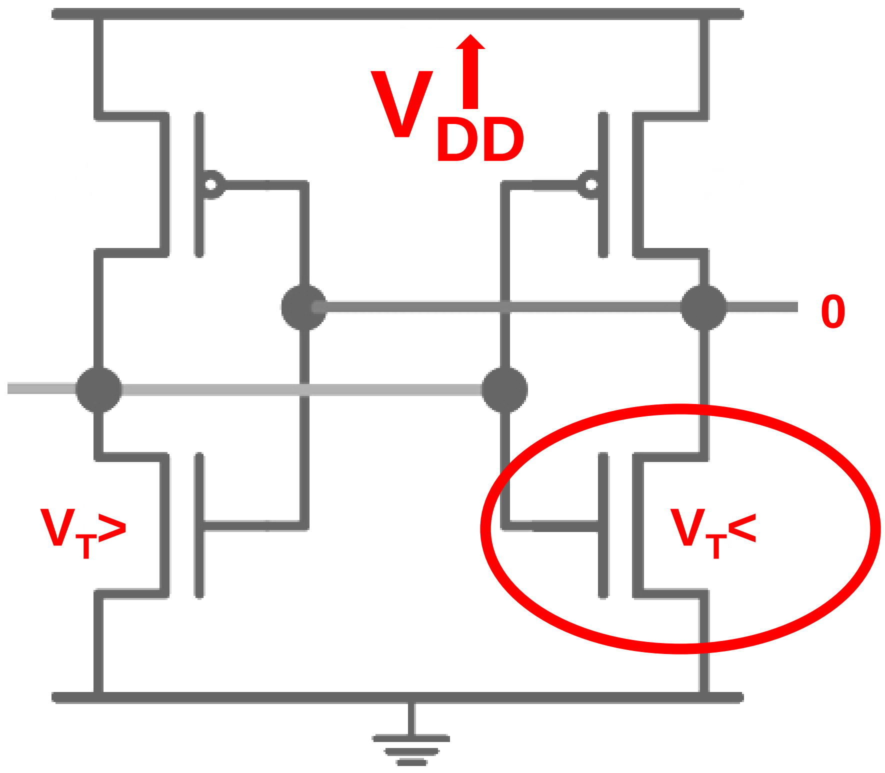


Pro's	Con's
Constructed from standard CMOS components	Limited set of C/R-pairs

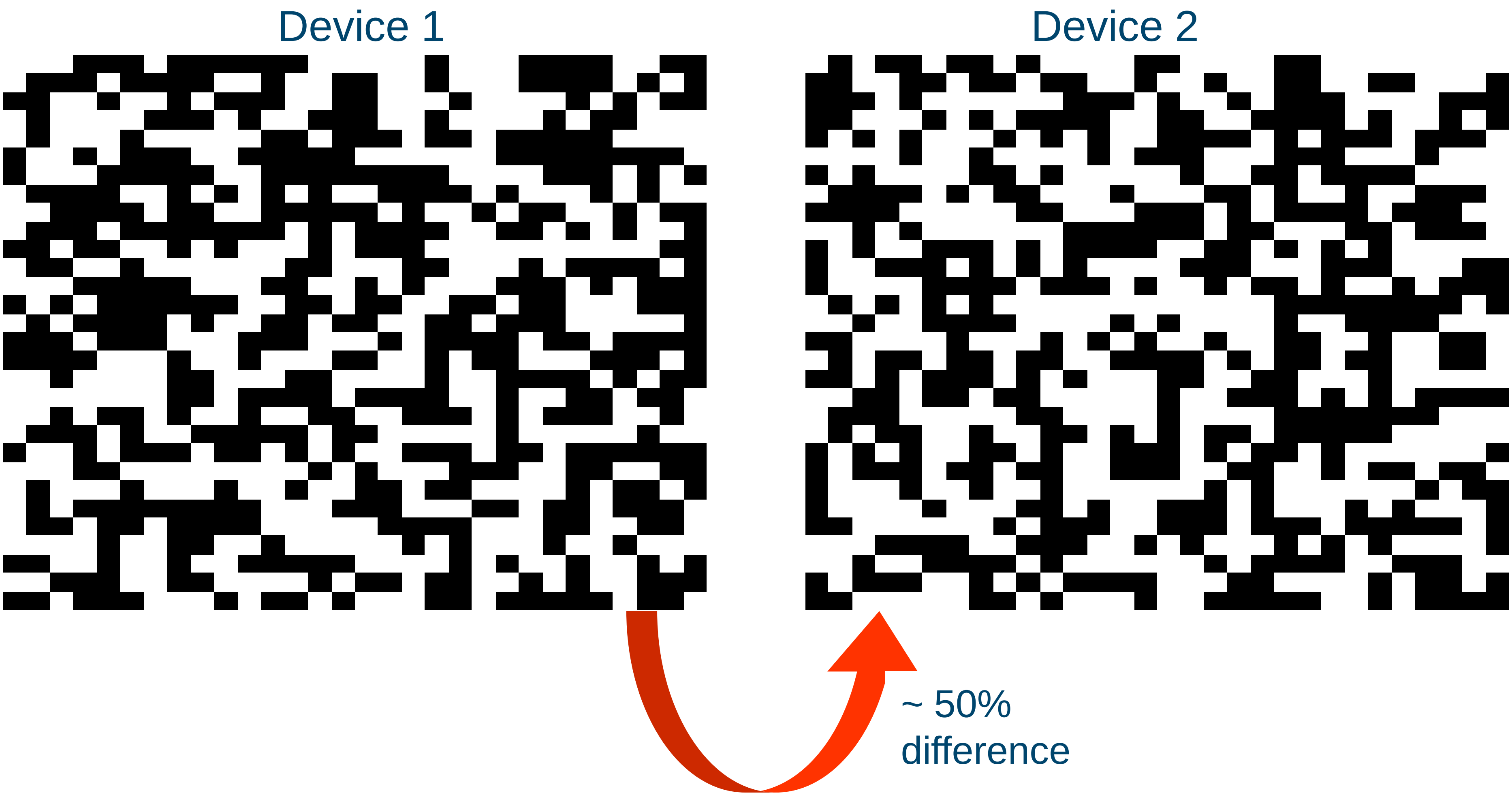
Example: SRAM memory cell (6T)



SRAM startup behavior



SRAM Uniqueness



SRAM Noise

~ 10% errors

Table of Contents

- Introduction
- PUF type analysis
- Use case for PUF technology
- Testing of PUF behavior
  - PUF Reliability
  - PUF Uniqueness
- Additional PUF research examples at Intrinsic-ID

Application: Secure Key Storage

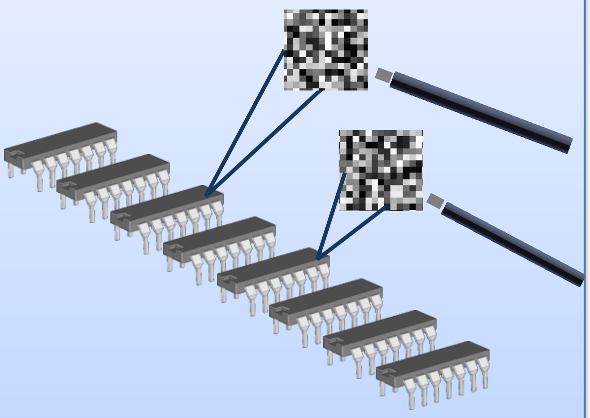
Known key storage options:

Fuses, E(E)PROM, Flash, Battery backed RAM, ROM, etc.

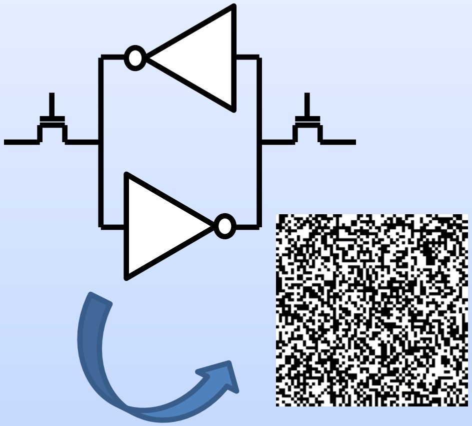
Problems of these methods:

- Security
- Costs
- Availability
- Time to Market

Hardware Intrinsic Security (HIS)



Due to deep sub-micron process variations ICs are intrinsically unique



Start–up SRAM values establish a unique and robust fingerprint

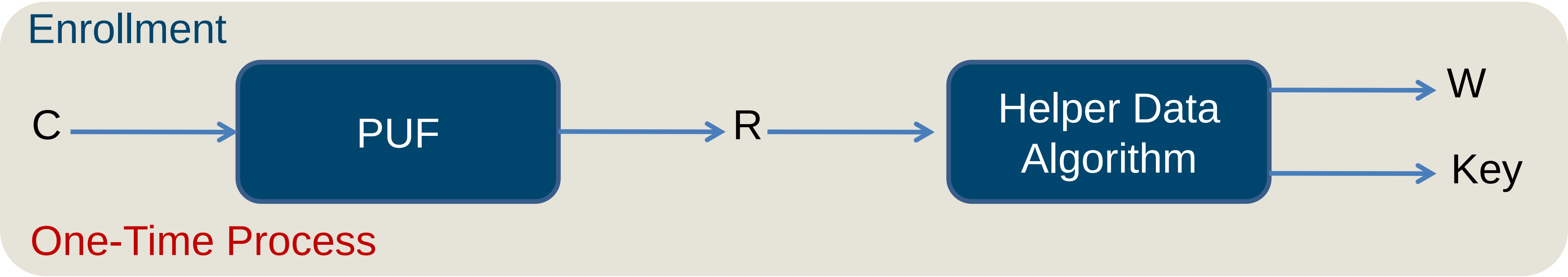
The electronic fingerprint is turned into a secure secret key, which is the foundation of enhanced security

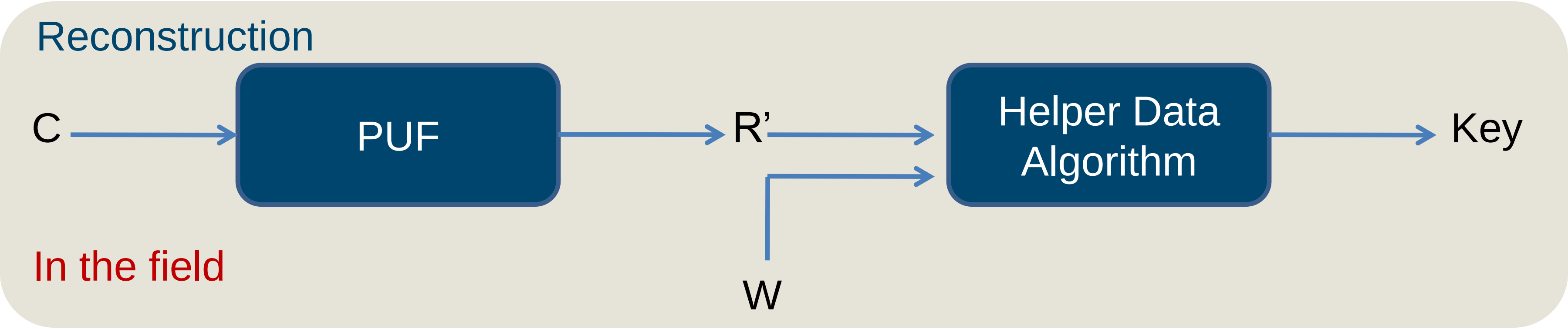
Security advantages of HIS

In order to protect keys against physical attacks:

1. Do not permanently store a key in non-volatile memory
2. Generate the key only when needed from a Physical Unclonable Function (PUF) in the IC
3. Delete the key

Key Storage With PUFs

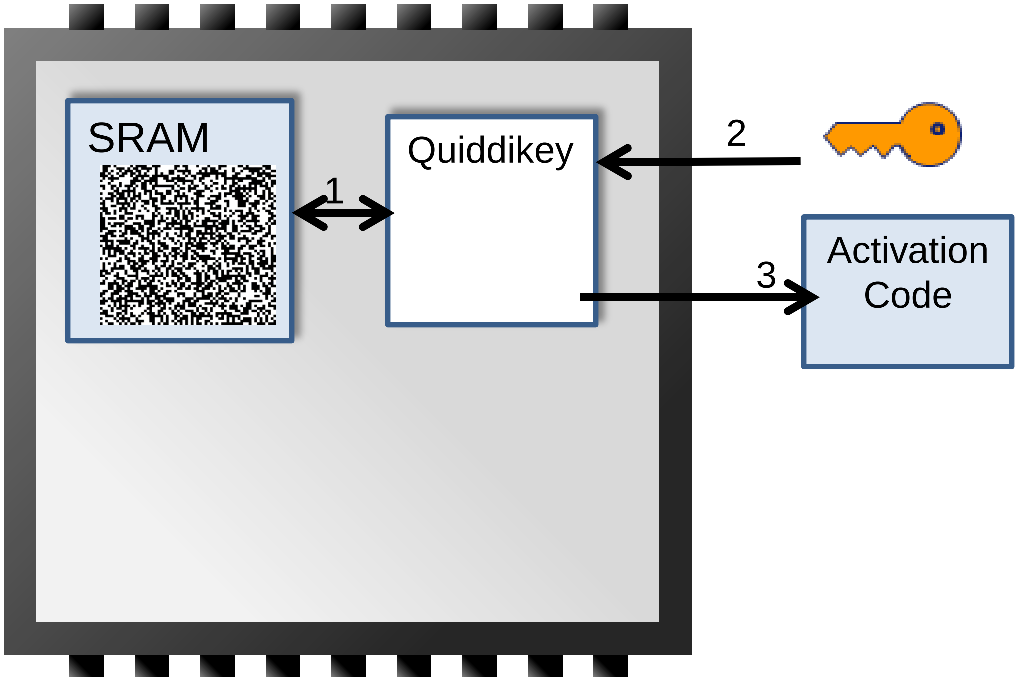




$I(W,Key)<\varepsilon$ $P[\text{Key not Correct}]<\delta$

Quiddikey™ Product, Key Programming

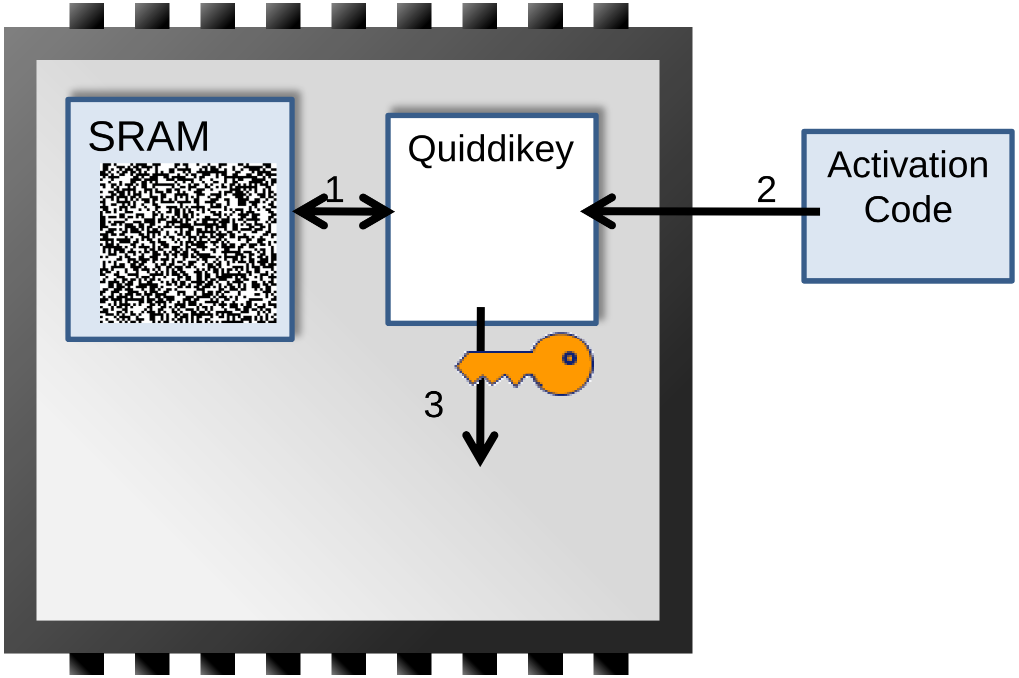
- Functionality
  - Storage of unique device keys
  - Storage of user keys
  - Key storage for AES, RSA, ECC
- Requirements
  - Uninitialized SRAM
  - Storage for device-unique activation code



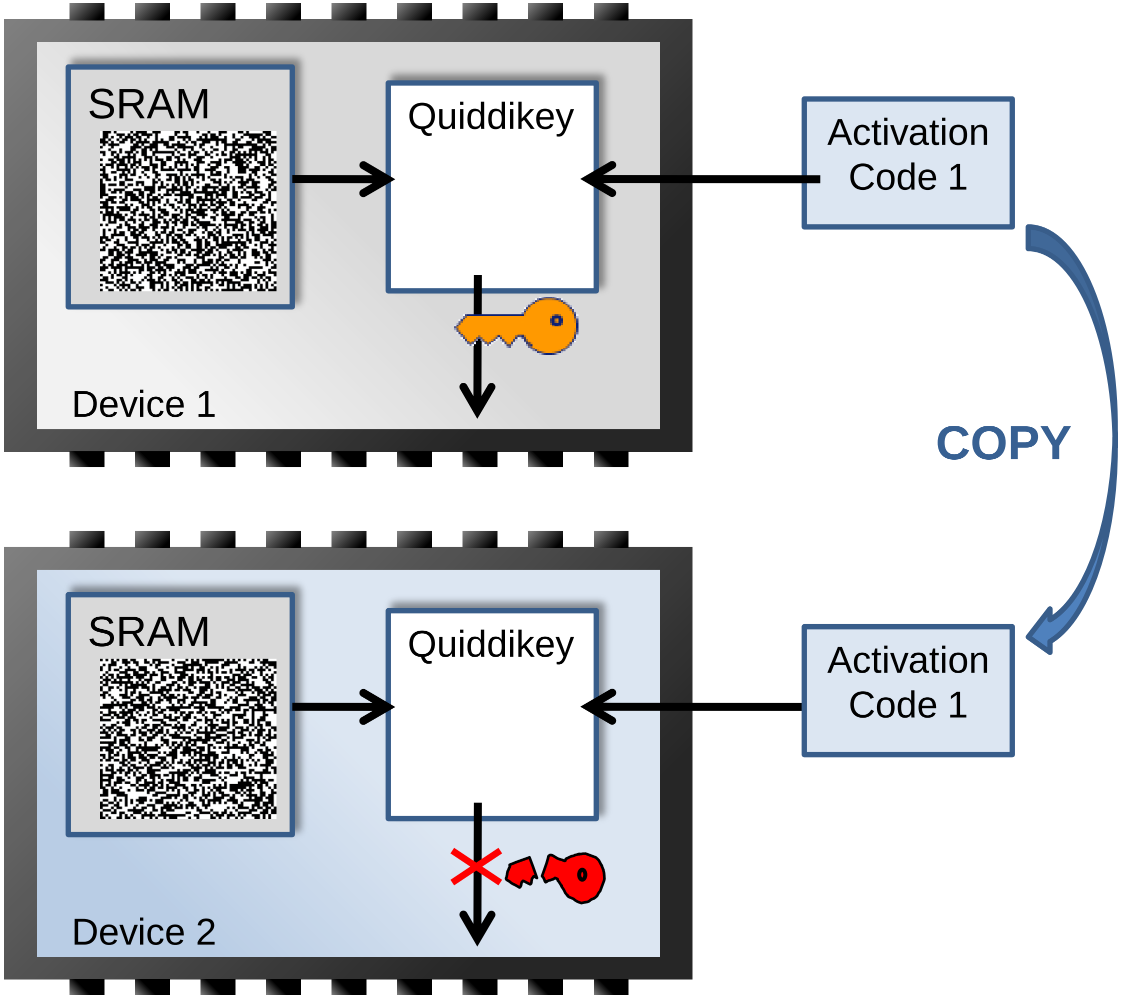
Quiddikey™ Product, Key Reconstruction

- Functionality
  - Storage of unique device keys
  - Storage of user keys
  - Key storage for AES, RSA, ECC

- Requirements
  - Uninitialized SRAM
  - Storage for device-unique activation code



Anti-cloning property



Confidentio™-SC

- Integrated security processing unit:
  - Secure key storage
  - Content / data encryption
  - Randomness generation
- Root of trust for mobile apps
- Targets SIM/SmartCard, Secure Digital (SD-) card or embedded Secure Element
- Complementary to
  - ARM TrustZone
  - GlobalPlatform Trusted Execution Environment (TEE)

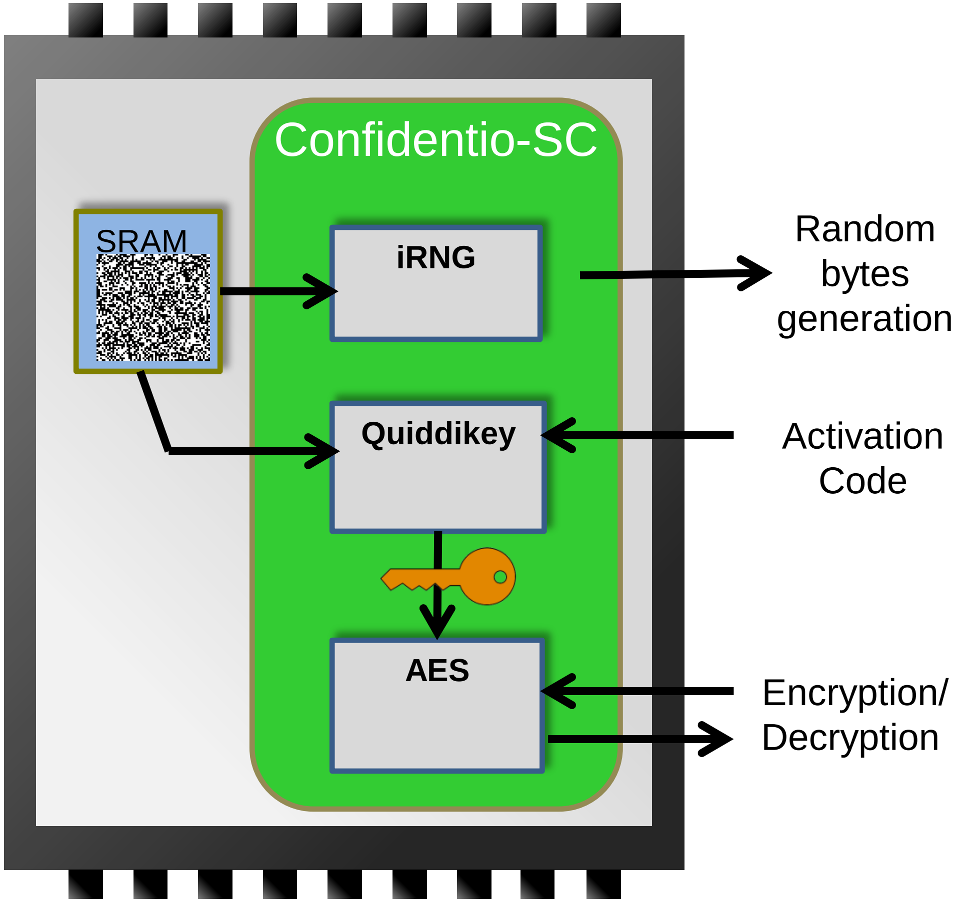


Table of Contents

- Introduction
- PUF type analysis
- Use case for PUF technology
- Testing of PUF behavior
    - PUF Reliability
    - PUF Uniqueness
- Additional PUF research examples at Intrinsic-ID

SRAM PUF test results

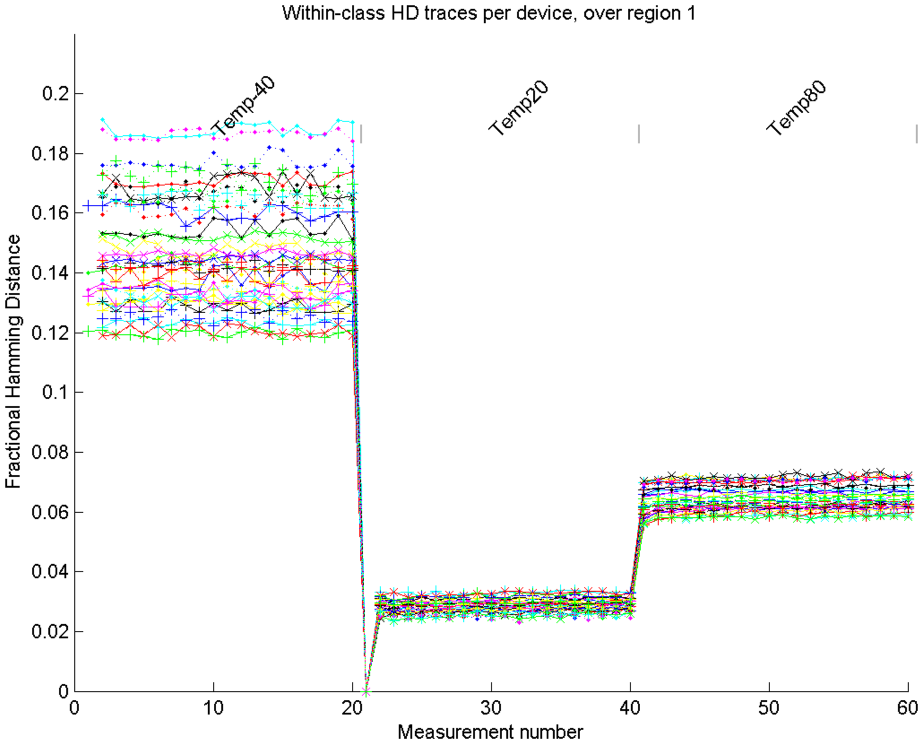
- Evaluation properties:
  - Reliability: when PUF responses are measured, the reference measurement should be recognized which was taken at enrollment
  - Uniqueness: PUF responses of a specific device are random and unpredictable, even given all PUF responses of other devices
- Studied SRAM instances from different technology nodes and vendors. Each SRAM memory was evaluated using the following tests:
  - Temperature Test (reliability)
  - Voltage Variation Test (reliability)
  - Hamming Weight Test (uniqueness)
  - Between-Class Uniqueness Test (uniqueness)
  - Secrecy Rate & Compression Test (reliability + uniqueness)
- Publication: **"Comparative analysis of SRAM memories used as PUF primitives"**, published at DATE 2012 (March 2012)

INTRINSIC ID

Secure your digital life™

Temperature Test

- Study stability of start-up values at different temperatures
- ICs measured under varying ambient temperature
- Measurement at 20˚C has been used as reference



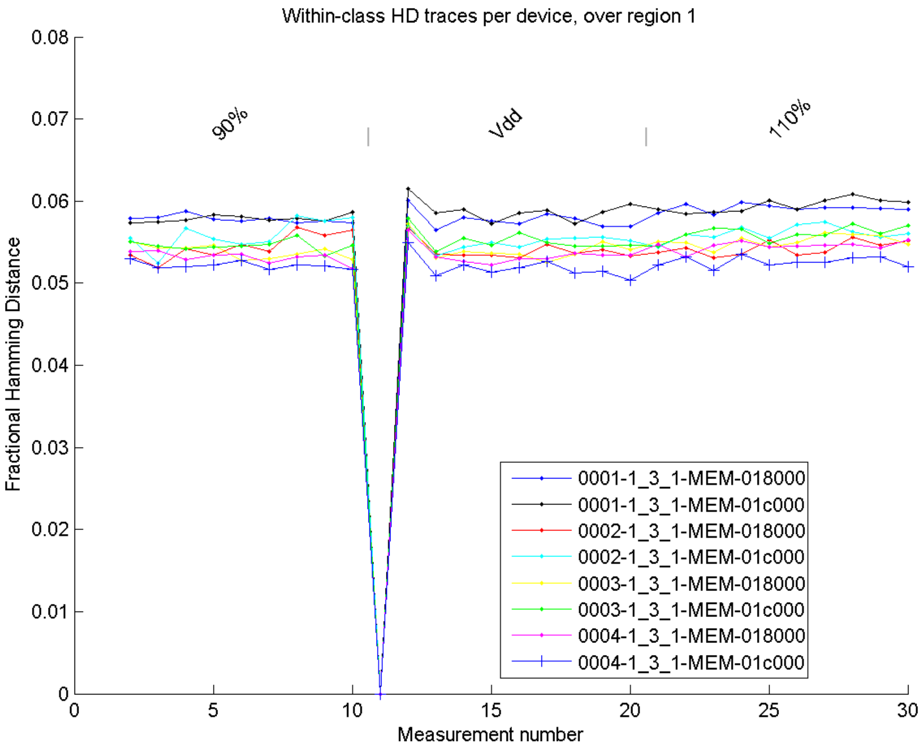
SRAM	Technology	Devices	−40°C			20°C			+80°C		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15632KV18	65nm	10	5.8%	7.8%	12.2%	3.3%	3.8%	4.3%	6.1%	6.6%	7.1%
Virage HP ASAP SP ULP 32-bit	90nm	34	11.5%	14.8%	19.6%	2.2%	2.9%	3.5%	5.0%	6.5%	8%
Virage HP ASAP SP ULP 64-bit	90nm	34	9.6%	11.8%	17.6%	2.6%	3.5%	4.0%	5.6%	7.7%	17.0%
Faraday SHGD130-1760X8X1BM1	130nm	40	8.4%	10.3%	13.7%	3.6%	4.5%	5.4%	6.7%	9.0%	13.0%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	9.3%	12.0%	19.6%	3.2%	4.8%	5.7%	7.0%	10.5%	20.5%
Cypress CY7C1041CV33-20ZSX	150nm	8	5.8%	6.7%	7.5%	2.9%	3.5%	3.9%	7.1%	8.0%	9.2%
IDT 71V416S15PHI	180nm	8	5.4%	6.0%	6.8%	2.3%	2.8%	3.3%	7.6%	8.4%	9.3%

INTRINSIC ID

Secure your digital life™

Voltage Variation Test

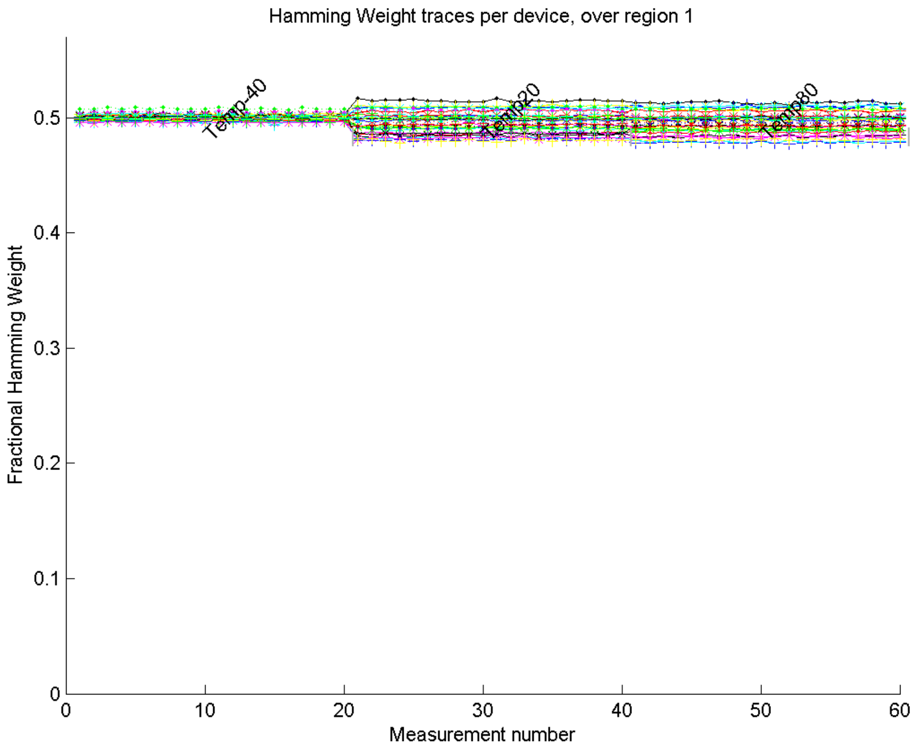
- Study stability of start-up values under variations of power supply voltage level
- Measurement at Vdd has been used as reference
- Hamming Distance during test very low and constant



SRAM	Technology	Devices	90% of Vdd			Vdd			110% of Vdd		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15632KV18	65nm	10	3.3%	3.9%	4.4%	3.4%	3.8%	4.4%	3.4%	3.8%	4.5%
Virage HP ASAP SP ULP 32-bit	90nm	8	5.0%	5.5%	6.0%	4.9%	5.5%	6.2%	5.1%	5.5%	6.1%
Virage HP ASAP SP ULP 64-bit	90nm	8	4.9%	5.5%	6.2%	4.9%	5.5%	6.3%	4.9%	5.6%	6.2%
Faraday SHGD130-1760X8X1BM1	130nm	10	4.0%	4.6%	5.2%	4.0%	4.6%	5.4%	3.9%	4.7%	5.4%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	10	4.0%	5.4%	6.3%	3.7%	5.5%	6.2%	3.9%	5.5%	6.4%
Cypress CY7C1041CV33-20ZSX	150nm	8	3.2%	3.5%	3.8%	3.1%	3.5%	3.9%	3.1%	3.5%	3.8%
IDT 71V416S15PHI	180nm	8	1.6%	1.8%	2.0%	1.5%	1.7%	1.9%	1.7%	1.9%	2.2%

Hamming Weight Test

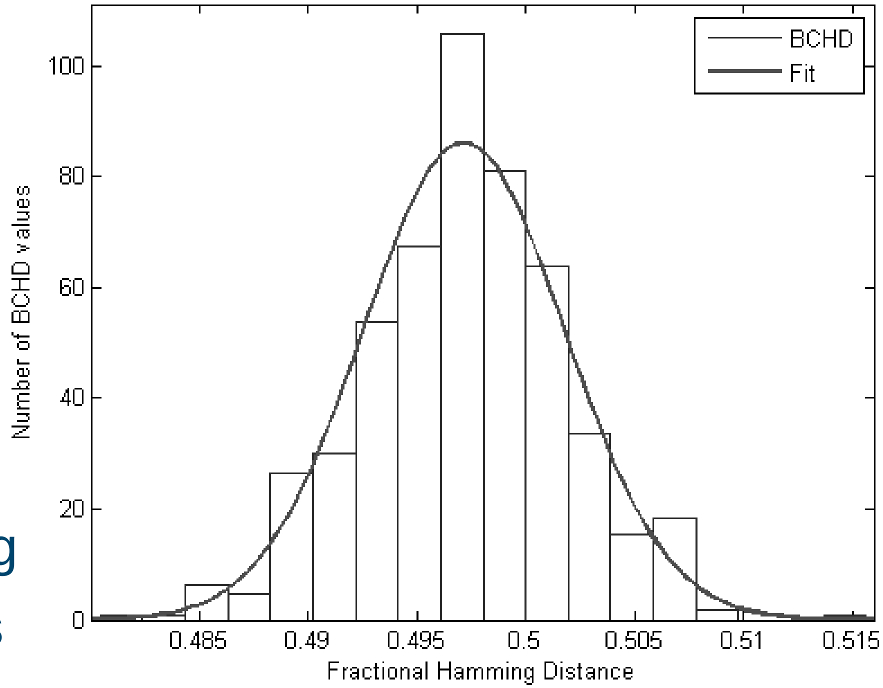
- Study uniqueness based on Hamming weight as well as stability at different temperatures
- ICs measured under varying ambient temperature
- Hamming weight during test around 50% and constant over temperature for most devices



SRAM	Technology	Devices	−40°C			20°C			+80°C		
			Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Cypress CY7C15634KV18	65nm	10	48.6%	49.6%	50.8%	48.6%	49.7%	50.7%	48.6%	49.9%	51.1%
Virage HP ASAP SP ULP 32-bit	90nm	34	48.7%	49.8%	51.1%	47.0%	49.3%	51.3%	46.8%	49.2%	51.1%
Virage HP ASAP SP ULP 64-bit	90nm	34	48.5%	49.6%	50.6%	48.0%	49.2%	50.6%	47.5%	48.9%	50.9%
Faraday SHGD130-1760X8X1BM1	130nm	40	49.2%	51.3%	54.0%	50.1%	53.5%	58.9%	49.9%	55.9%	65.2%
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	48.7%	50.0%	51.1%	49.1%	50.1%	51.1%	48.9%	50.0%	51.2%
Cypress CY7C1041CV33-20ZSX	150nm	8	48.1%	50.0%	51.0%	49.1%	50.1%	51.1%	49.3%	50.1%	51.1%
IDT 71V416S15PHI	180nm	8	40.4%	42.1%	43.4%	40.5%	42.1%	43.5%	40.4%	41.9%	43.6%

Between-class Uniqueness Test

- Study uniqueness based on between-class HD distributions
- Hamming Distances should be Gaussian distribution with mean at 0.5 and small standard deviation
- Results very good for devices that also had good results in Hamming Weight Test, less for devices with bias



SRAM	Technology	Devices	Number of BCHD values	μ	σ
Cypress CY7C15634KV18	65nm	10	(10*9)/2 = 45	0.500	0.0033
Virage HP ASAP SP ULP 32-bit	90nm	34	(34*31)/2 = 496	0.497	0.0046
Virage HP ASAP SP ULP 64-bit	90nm	34	(34*31)/2 = 496	0.496	0.0043
Faraday SHGD130-1760X8X1BM1	130nm	40	(40*39)/2 = 780	0.467	0.014
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	(40*39)/2 = 780	0.451	0.023
Cypress CY7C1041CV33-20ZSX	150nm	8	(8*7)/2 = 28	0.499	0.0034
IDT 71V416S15PHI	180nm	8	(8*7)/2 = 28	0.486	0.0041

Secrecy Rate & Compression Test

- Direct CTW compression test indicates that worst-case there is only small amount of non-randomness in PUF responses (compression to 98.2%)
- Context-Tree Weighting (CTW) algorithm was used to estimate the mutual information between PUF responses: I(X) = H(X) – H(X | X')
- Mutual information provides maximum achievable secrecy rate, which determines amount of compression needed for privacy amplification
- Worst-case mutual information found is 0.38 (Virage HP SRAM)
- Worst-case required compression factor is therefore 1/0.38 = 2.6

SRAM	Technology	Devices	Compressed size (bits)	Original size (bits)	Compression ratio	Minimum I(R,R')	Average I(R,R')	Maximum I(R,R')
Cypress CY7C15632KV18	65nm	10	16392	16384	100.0 %	0.62	0.64	0.65
Virage HP ASAP SP ULP 32-bit	90nm	34	16385	16384	100.0 %	0.38	0.59	0.69
Virage HP ASAP SP ULP 64-bit	90nm	34	16389	16384	100.0 %	0.49	0.63	0.73
Faraday SHGD130-1760X8X1BM1	130nm	40	13896	14000	99.3%	0.52	0.61	0.69
Virage asdsrsnfs1p1750x8cm16sw0	130nm	40	13903	14000	99.3%	0.47	0.57	0.67
Cypress CY7C1041CV33-20ZSX	150nm	8	16392	16384	100.0 %	0.60	0.70	0.76
IDT 71V416S15PHI	180nm	8	16091	16384	98.2%	0.57	0.70	0.79

Fuzzy Extractor Design

- Design goal: derive 128-bit cryptographic key with failure rate $<10^{-9}$, using worst-case secrecy rate (0.38) and noise (21%) assumptions
- Amount of secret bits required = 128/0.38 = 337
- Concatenated error-correcting code design that achieves failure rate $< 10^{-9}$ assuming 21% noise:
  - Inner code: 3x BCH-code [n,k,d]=[255,115,43]
  - Outer code: 765x Repetition-11 code
- This design requires 1.03KB of SRAM memory

Reliability tests performed at Intrinsic-ID

- Tested: 180, 150, 130, 90, 65 nm
- Temperature cycle / temperature ramp
- Endurance low temperature: IEC 60068-2-1
- Endurance high temperature: IEC 60068-2-2
- Radio frequency electromagnetic field: IEC 61000-4-3
- Ambient electromagnetic fields immunity: EMC: EN55020
- Electromagnetic compatibility
- Humidity
- Voltage ramp-up
- Data retention voltage
- Accelerated lifetime
- Extensive End customer validation
- Millions of measurements performed

Photo: Philips Innovation Services

Table of Contents

European research projects

- PUFFIN
  - Providing intrinsic and long-wanted basis for security in everyone's most common computing platforms: PCs and mobile devices
- RELY
  - Targeting reliability as parameter throughout chip development
- UNIQUE (finalized in 2012)
  - Tackling counterfeiting of and tampering with Integrated Circuits
- RATE
  - Dutch project focused on modeling impact of process variations, environmental parameters and ageing on SRAM PUFs

Some selected papers from Intrinsic-ID

- **Using PUF noise for random number generation**
  - **"Efficient Implementation of True Random Number Generator based on SRAM PUFs"** in Cryptography & Security: From Theory to Applications, 2012
- **Soft decision error correction (decreasing required SRAM)**
  - **"Soft Decision Error Correction for Compact Memory-Based PUFs using a Single Enrollment"** at CHES 2012 conference
- **New type of memory based PUF: Buskeepers**
  - **"Buskeeper PUFs, a Promising Alternative to D Flip-Flop PUFs"** at HOST 2012 workshop
- **Re-usable PUF: Logically Reconfigurable PUF**
  - **"Recyclable PUFs: Logically Reconfigurable PUFs"** in Journal of Cryptographic Engineering, November 2011 and at CHES 2011 conference
  - **"Logically Reconfigurable PUFs: Memory-Based Secure Key Storage"** at ACM STC 2011 workshop

INTRINSIC ID

Secure your digital life™