

Hardware Security: Investigation of Fingerprinting (Advanced CMOS and PCB level)

Matthias Ludwig, Vincent Krämer 2024-03-20



Table of contents





infineon

Table of contents



Introduction





Secured hardware is vital for system-critical applications



Hardware fingerprints claim to enable realizing security goals such as anti-counterfeiting, secured key storage, or authentication



Evaluating the **claimed property** that fingerprints are **protected from being reproduced** by direct physical characterization



Introduction: Fingerprinting

Example: Ring Oscillator

Equally designed and only influenced by randomly occurring manufacturing variances





Background & Research Question

Observing – Side-Channel

"Side-Channel Analysis of 'PUFs' and Fuzzy Extractors"

"Localized electromagnetic analysis of RO 'PUFs'"

[1], [2]

$\widehat{\mathbf{o}}$

Semi-Invasive – Optical

Attacks on 'PUFs' by photonic emission analysis

Identification of fingerprints by correlation optical images and emission fingerprints

[3], [4]



Demonstrated a Focused Ion Beam circuit edit with which they produced a physical clone of their Proof-of-Concept SRAM 'PUF' implementation

[5]





Research question: Can hardware fingerprints be effectively characterized by direct physical measurement methods?



Physical Model

To effectively characterize fingerprints, we need a **link between hardware and response**



Research Agenda







Case Studies



Table of contents







Recap: Start-Up SRAM Cell





Ground Truth Generation & Evaluation





Delayering and Imaging (RE) of the ROI



anabaitai	popopogogog	19050505	i foi foi foi foi foi foi	boro boro hoi	5050505	05050505	1511501	Andrew Production Pro-			
hikak	into konto hono	Roza Roza	bo ko ko ko ko k	a ha ha ha ha ha ha	Bogo Bogo	habakaka	Robok	a ko ko ko ko ko kom			A REAL PROPERTY AND A REAL
i a la c		a si si si si si	4.4.4.4.4.4.	and a solution	indridia.	a la	and and and	Contratation for			
23,322		1912111		12121232	1212123	197835378	23232	323233232323233 3 00			Conceptual designed and the second
aboritori de	silonko koriko ilo	pagagaga	04522200000	agagagagaga	alkalkalka	kokokoko	Babab	o po po po po po poro			the second se
agagai	hu ka ka ka ka k	ດຊີດຊີດຊີດຊີ	າວິດສີຍີວິດຊີບຊີບ	percenser and	la la la la	agagagag	ngagai	ka k			1 A. A.
Sec. in	1.1.1.1.1.1.1.1.	Auto Balan	and a standard and a stand of the	abababababa	-labola	Patataka	Sabah	aperater aperator			the second se
323233	1111111	32723274		111111111	111111	12727272	232321	223232323252520		And and the second second	and the second se
	Contractor for for the state	111111	-fofferfofferfo	fofofofofofof	0.1.00	10111111	24282				the second s
ilio ilio ilio	nijo ijo ijo ije ije	gagagaga	φοιξοιφοιφαιξ	agagagagaga	sgogoga	fozafozo	Babab	apapagagagagagag			Contraction of the local division of the loc
ababas	la ka ka ka ka k	akakakak	- Rokokokokoko	Radadadada	la ka ka k	okokokak	in Ro Ro s	Logogogogogogogo	1.000		· · · · · · · · · · · · · · · · · · ·
and a	and and the	Assessed and	Constant and a start	abatatatat	202020	Parata Para	Rabate	nininininininini			
32313	1343131313333	36323637			2525282	7,3,3,7,2,7,2	32323	15252525252525		A	and the second se
o go go j	ballankalkalkal	o de la de de la	albolite ka lita iba	BoBoBoBoBoBo	0.00.000	afferfafferf	of a feature	Collecter Collec	-		the second se
iĝoĝoĝe	သိုဂနိုင်ဆိုင်နိုင်ဆိုင်	ijožožožo	វុកព្រំហៀកវ៉ុកស៊ីកស៊ី	a ka da ka ka ka ka	specesja	konakana	zozoze	o go			I COMPANY AND ADDRESS OF THE OWNER
adridad	la kakakakak	- 2-2-2-2-2	- Rokokokokoko	ພື້ອສິກສິກສິກສິກສິກ	Libritrit	ohahahat	adadai	to hat a so had a so had a so		1000	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O
121.2	3. 6. 6. 6. 6. 6.				1212233	1.1.1.2.2.2.1	82423	507072525252 50			Contraction of the local division of the loc
3.3.3	21212723232	1.1.1.1.1.1.1		232325232	2323252	82828282	82828	10 10101252525	- B	1678	
ogener	çe içe içe içe içe iç	agagagag	n se	pagapakaka	baike kaik	0.000.0000	oliolio:		-	LOTO	
dododo	ago go go go go	Budadada	ໃດທີ່ກ່ຽວຊີດຊີດຊີ	aganonangan	ožožoža	kakakaba	808080	o P. Tako kaka kato			
anakai	to bo bo bo bo bo	alebalah	in to both to both	Sala Laka tak	Labarate.	o Bollo Boll				CONTRACTOR OF	and the second se
22.32	1111111111111	1212122	101010120101	12112220222	1121122	10111111	38,833	000000000000000000000000000000000000000			and the second se
Series Series	- Borberbuilte	Sugarouters	beren for beren for	opopopopop	SPOROFIC .	50505050	20202	2525252525252520			and the second sec
agagat	ço ço şağaşaşa	ngegageg	akakekakeka	gagagagagag	ça ga ga ga	ogogogog	0.80.803	to popolo popolo po			And the second se
Sidis	i ha ha ha ha ha ha	ho ho ho ho	bolton konkonkonk	alle halle hall	a ha ha ha ha	Radadada	Ratak	and of a factor of a factor of a	•		
222.2		10.0.0.0	52525352525	1.1.1.1.1.1.1.1.1	i santa k		ليقتدفن			-	and the second s
131332	1252325252525	2323232323	2713232323232	0452023202	1282828	251511125	232303	125252525252525250			NAME OF TAXABLE PARTY.
99999	service and the second	gano gana	ga ga ga ga ga ga ga g	nga kasasasa	ogagaga	Bulbabulba	Sold of	akakakakakakaka			the second se
o ko ko	la l	ngagagag	idadadada	grild grild go go go	<u>faifaitaita</u>	olokokak	ngogoi	20202020202020	-		and a restaurant of the second s
Same	ala bahahala	de de de de	la hababababab	a kaka ka ka	a ka ka ka	hononan	Labore	akakakakakakaka		*	•
3,3,3	12723232523	33332333	12222221222	4-27672340	6767676	18121819	38282				COLUMN TWO IS NOT THE OWNER.
03033	532323232323			1252125252	1212723	10202020	23232	120202020202020			the second se
igo go go	oritor itorita il oritori	gagagagaga	iju ijo ija ija ijo ijo ij	alia kalialialia	ogogogo	Raikakaika	90.00.9	a Eo So So So So Solo			The second se
o failer	la kaimila kai	adaman	anananananan	La La La La La La	lakakak	ožožožož	n Rozofi i	pollogododogodo		And the second	Contraction of the second states of the second stat
12223		12121212	2282828282828	ala la faila la fa		2. Contration	22222		•		
3,32,3	191919193	3,33,32,32	1012121212120	000000000000000000000000000000000000000	10111111	72127272	32525	25252525252525	-		And a state of the
66587		07050707		100000000000000000000000000000000000000		27272728	33333	50125252525250			And the second s
Burgersh	nije izvije konzo	ijuijaijuijo;	ija ko ko ko ko k	espinopolpolp	ogogogo	hahahaha	hohoh	a ga ga ga ga ga ga g		40	And I wanted to be a set of the s
hikadan	and a deriver and	ກສາກສາກິດສິ	a ka ka ka ka ka	RobertoReal	lakakak	akakakak	nibided	Bailo Ro Bo Ro Reiko	contra de	3	
3.2.2.6	12022-02022	1242424	12121222	0.11112	and and	37373737	123225		Concernance of the local division of the loc	See	
3,3,3	25454545454	02020202	3232323232323	0000000000000	27,27,27,2	72525255	0,00,0	15151515252525252			
e gagai	ga ga ga ga ga ga ga ga	engengengeng	a paga paga paga pa	ala da barbarbarbar	a fa fa fa	anonanan	19090		-		and the second se
andra	alaria da hala	Reifeileila	κολοφούρα	adadadadad	o Ro Ro Ro	Roza Roza	Roborge	and a set of			
64242		a to the second		antribotorio	2020202	alaintai	and the second	interimental			A REAL PROPERTY AND A REAL
23372		CONTRACTOR STREET	11123333333	022222202	1474247	000000000	30303				the second se
3.8.3		20201020		151517575777		3-2-3-2-1-3	82323	13,3,3,3,3,3,3,3,2,00		Contraction of the local division of the loc	
janja njeo	gang-mangangang	ageignigeg	alakokakaip	delle delle de	(agana)	no papagos	anganga)	porporpor por por por por			1 1.1 1.4
	Sugar Huderson	Sector Land	ale hate her	andring	Andrika	holohoho	de ma	and a standard and a			
and the		10.000	14747424727	10 10 10 10 10 10 10 10 10 10 10 10 10 1	7232/3	24242424	ale in	and a state of the			And Annual Property of the owner
	1414540412			Calle La La La	434344	1.11.1	32374	a faile faile faile			the second se
State of the	10/10/10/10/10	the second second	and the second	And the second second	Carl Street	CONC.	1000	A CONTRACTOR OF THE OWNER			the second se
ALC: NO		1		W	31						The second se
	and the second se	and the second second					-		3		A . A . A
202	HV	curr	mag 🖽	WD	det	mode	tilt				
796											
000	1.00 kV	50 pA	6 500 x	4.1 mm	TLD	SE	0 °				
										-	







Physical Model Generation [7]



Measurement and Data Analysis: Probing (WIP)



- Place nanoprobes on transistors
- **Output:** Voltage transfer characteristics
- Preferred cells is evaluated by equation from [6]
- **Does not scale** for many cells





Measurement: Layout

 Allows to measure length/width of transistors automatically

- Transconductance and, ultimately cell state depend on
 - Oxide thickness
 - Transistor geometry (L/W)
 - Doping parameters

- Only parameters length/width available in layout analysis

$$\beta_i = \frac{1}{2} \cdot \mu_i \cdot \frac{\varepsilon_0 \cdot \varepsilon_{r,ox}}{d_{ox}} \cdot \frac{W}{L}$$







Data Analysis: Layout (WIP)

- Cells are detected by image processing (red)
- Width/length of transistors (green)

Cell	Transistor	L [nm]	W [nm]	Ground truth
	M1	62	116	
$\mathbf{C}0$	M2	60	71	1
CO	M3	58	63	1
	M4	61	116	
	M 1	61	119	
C1	M2	58	68	0
CI	M 3	58	66	0
	M 4	64	114	

- Find correlation between measurements and ground truth
- Preferred cells is evaluated by formula [7]



Table of contents







Overview



Physical Model Generation







Resistance Measurement: Electrical

Method	Resolution	Cost
Laboratory set-up (resistance) (Keithley Model 4200, KS PM8, 407B simac tips)	0.1μΩ, -	~100 000€
	$\begin{array}{c} \cdot 10^{-2} \\ 6 \\ 4 \\ 2 \\ 0 \\ 0 \\ 0.1 \end{array}$	PCB 1 PCB 2 PCB 3

Fig. 14: Electrical resistance measurement results.

11



Resistance Measurement: Optical









Fig. 14: Electrical resistance measurement results.



Both the **electrical** and the **optical** measurement **correlate** with the manufacturer values

Fig. 15: Geometrical max width measurement results.



Results of Capacitance Measurement: Electrical

Method	Resolution	Cost
Laboratory set-up (capacitance) (Andeen Hagerling 2700A, KS PM8, HM 7044, 407B simac tips)	-, 0.1 nF	~80000€





The measurement **correlates** with the manufacturer values

Table of contents





Conclusion





We propose a methodology to transfer hardware physics and responses into a physical model



Evaluation capability of hardware primitives' correlates to financial expenditure



Hardware design of fingerprints must take **reverse engineering / physical inspection** capabilities into account





Literature

[1] Merli, Dominik / Schuster, Dieter / Stumpf, Frederic / Sigl, Georg; **Side-Channel Analysis of PUFs and Fuzzy Extractors**; 2011; Trust and Trustworthy Computing; Springer Berlin Heidelberg; p. 33-47

[2] Merli, Dominik / Heyszl, Johann / Heinz, Benedikt / Schuster, Dieter / Stumpf, Frederic / Sigl, Georg; Localized electromagnetic analysis of RO PUFs; 2013-06; 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

[3] Tajik, Shahin / Dietz, Enrico / Frohmann, Sven / Seifert, Jean-Pierre / Nedospasov, Dmitry / Helfmeier, Clemens / Boit, Christian / Dittrich, Helmar; **Physical Characterization of Arbiter PUFs**; 2014; Advanced Information Systems Engineering

[4] Nedospasov, Dmitry / Seifert, Jean-Pierre / Helfmeier, Clemens / Boit, Christian; **Invasive PUF Analysis**; 2013-08; 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography; IEEE; p. 30-38

[5] Helfmeier, Clemens / Boit, Christian / Nedospasov, Dmitry / Seifert, Jean-Pierre; Cloning Physically Unclonable Functions; 2013-06;
2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)

[6] Cortez, Mafalda / Dargar, Apurva / Hamdioui, Said / Schrijen, Geert-Jan; **Modeling SRAM start-up behavior for Physical Unclonable Functions**; 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT); IEEE



Reasons for Manufacturing Variations

- Variations in Si0_2 Thickness
- Alignment of mask
- Variations in exposure / angle
- Variations due to distribution of etch liquid
- Variations in diffusion

- \rightarrow Process Parameters affected by Variations (Drennan et al. 2003):
- Electron / Hole Mobility $\mu n / \mu p$
- Flatband Voltage Vfb
- Substrate dopant concentration Nsub
- Gate oxide thickness tOx
- Length offset ΔL , Width offset ΔW , Short channel effect, Narrow width effect
- Source/drain sheet resistance



On-board measurement

- Evaluate the difference by operational amplifiers
- First differential amplifiers:
 - Put the voltage over R1/R2 to an single-ended output
- Second differential amplifier:
 - Amplify the difference to positive / negative value
- Gain is determined by R5/R3 (if R3=R4 and R5=R6)





On-board measurement

- Evaluate the difference by a schering bridge
- Difference of capacitance defines current flow through R1 resistor
- Operational amplifier increases this voltage
- Xor gate checks if signals are in phase
 - Produce stable 0/1 output

