



HAL
open science

Logic-Locking schemes and side channel attacks resilience

Nassim Riadi, Florent Bruguier, Pascal Benoit, Sophie Dupuis, Marie-Lise
Flottes

► **To cite this version:**

Nassim Riadi, Florent Bruguier, Pascal Benoit, Sophie Dupuis, Marie-Lise Flottes. Logic-Locking schemes and side channel attacks resilience. SAFEST Workshop, Jun 2023, Tallinn (Virtual), Estonia. lirmm-04526269

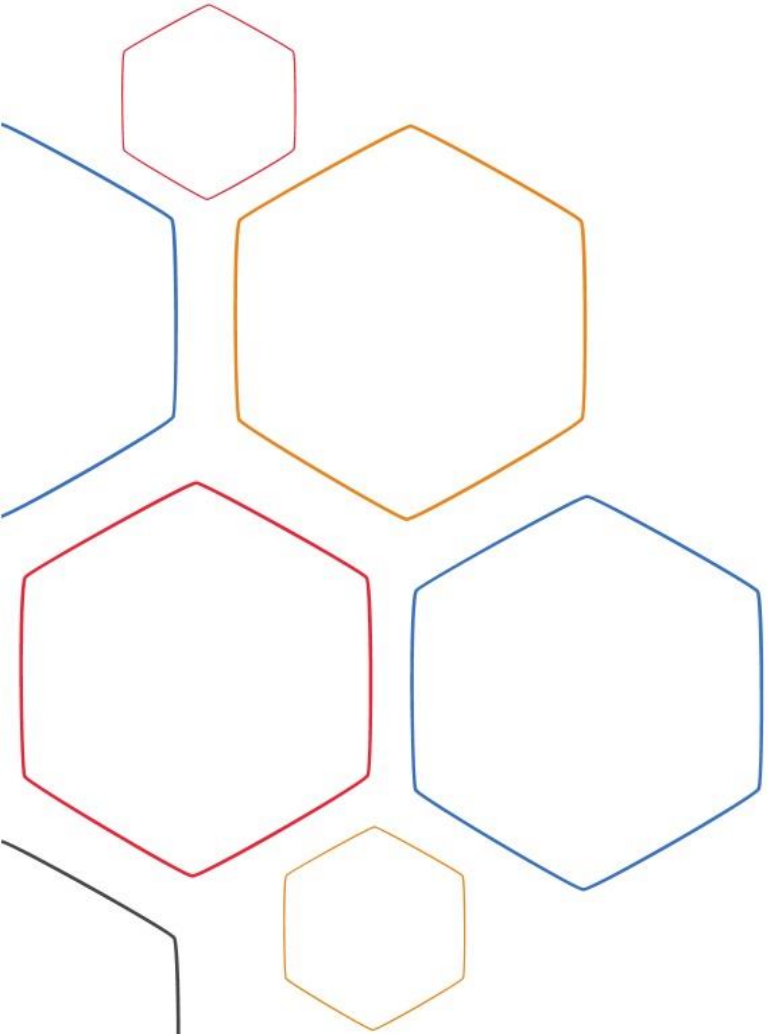
HAL Id: lirmm-04526269

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-04526269>

Submitted on 29 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Logic-Locking schemes and side channel attacks resilience

RIADI Nassim, PhD student

Thesis Director : Pascal Benoit

Thesis Supervisors : Florent Bruguier, Marie-Lise Flottes, Sophie Dupuis



LIRMM



19/06/2023



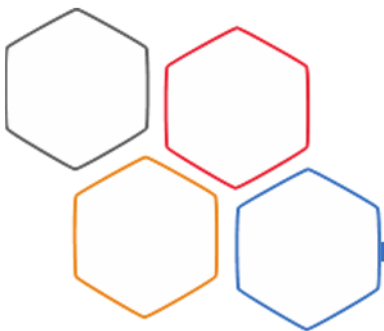
UNIVERSITÉ DE
MONTPELLIER



→ Logic Locking

→ SCA on Logic Locking

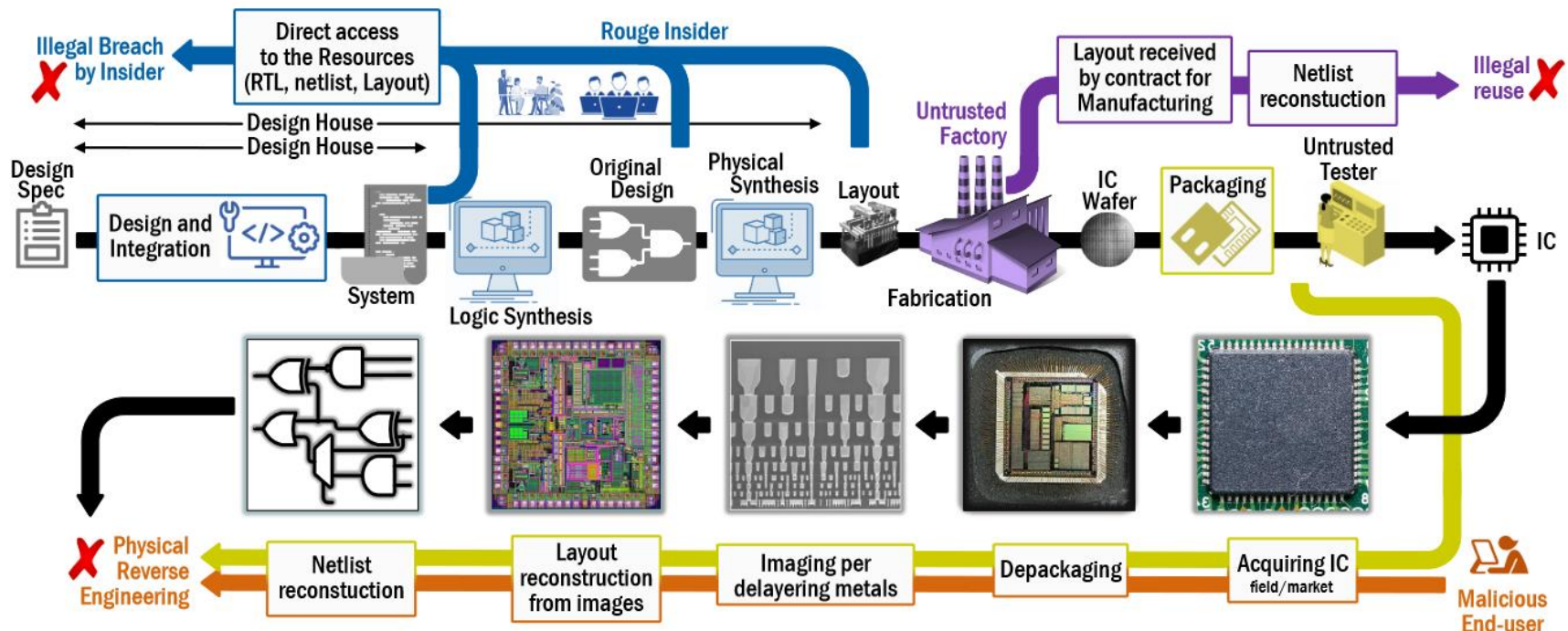
→ Perspectives



- Globalization of the IC production flow

- Threats

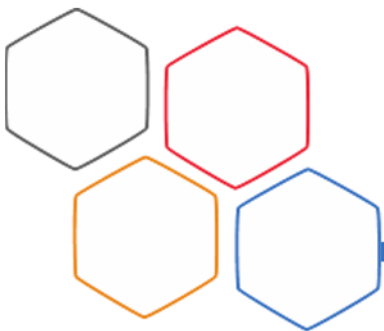
- IP piracy
- Counterfeiting
- Overproduction
- Reverse engineering
- Hardware Trojans



Threat models at different stages of IC production flow [1]

=> Development of solutions for the IP protection

[1] H. M. Kamali, K. Z. Azar, F. Farahmandi, et M. Tehranipoor, « Advances in Logic Locking: Past, Present, and Prospects », p. 39.



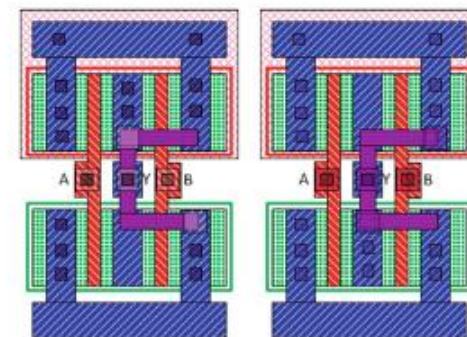
Logic Locking

DFTTr Solutions

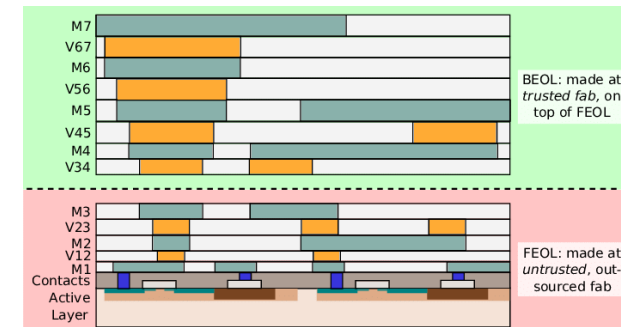
DFTTr (Design For Trust) e.g

- Camouflaging [2]
- Split-manufacturing
- **Logic Locking**

Threat level	Camouflaging	Split manufacturing	Logic Locking
Design team	No	No	Yes
Untrusted Foundry	No	Yes	Yes
End-user	Yes	No	Yes

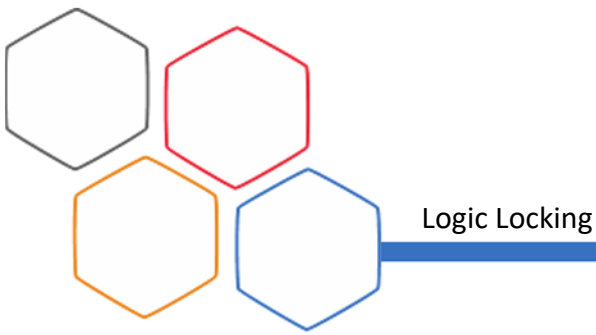


Camouflaging (NAND, NOR) [2]



Split-manufacturing

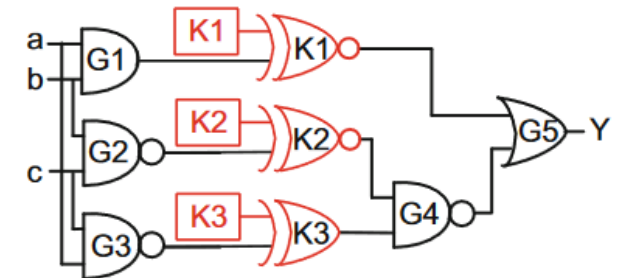
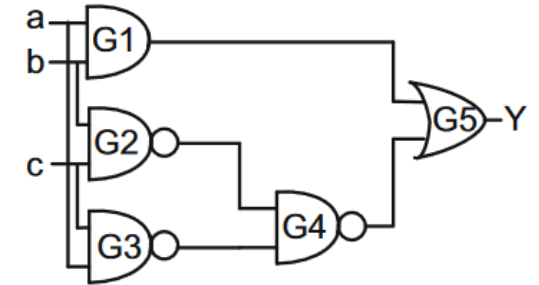
[2] M. Yasin, J. Rajendran, et O. Sinanoglu, Trustworthy Hardware Design: Combinational Logic Locking Techniques. Cham: Springer International Publishing, 2020. doi: [10.1007/978-3-030-15334-2](https://doi.org/10.1007/978-3-030-15334-2).



Logic Locking

The Logic Locking is a DFT technique which consists in locking the correct behaviour of the circuit with a secret key. $L(i, ks) = F(i), \forall i \in I$

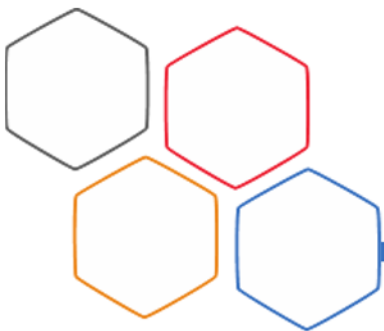
- F : Boolean function
- L : Locked boolean function
- Ks: Secret key



Evaluation Metrics :

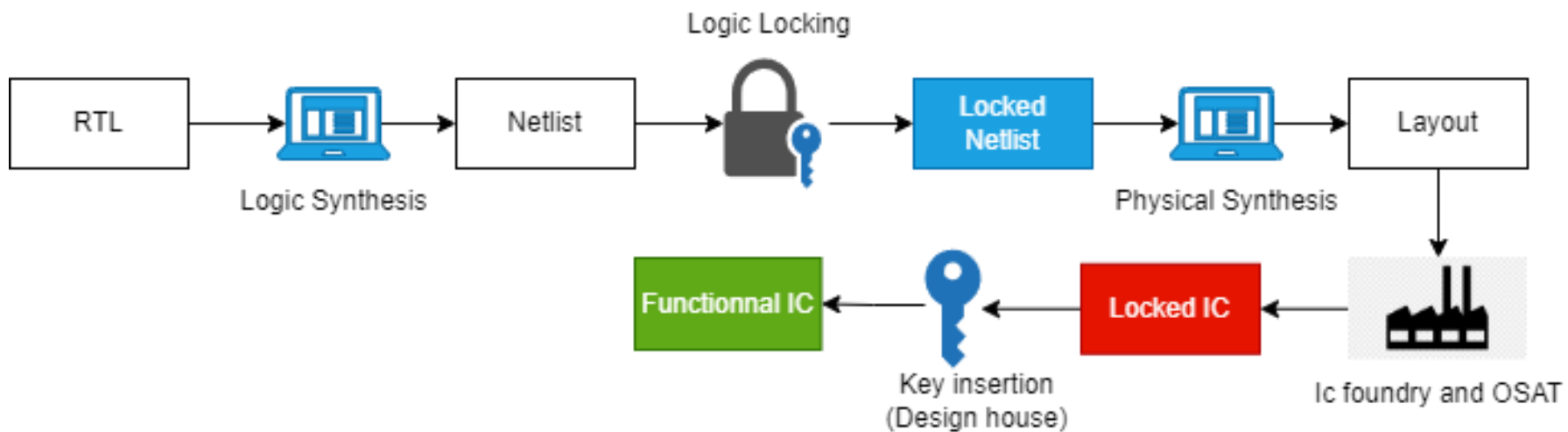
- Output Corruptibility :

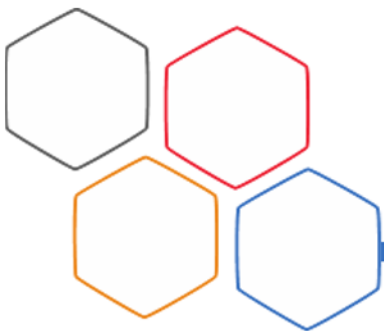
$$OC = \frac{1}{P \times Q \times M} \sum_{i=1}^P \sum_{j=1}^Q HD(O_F(I_i), O_L(I_i, K_j)) \times 100\%$$



Logic Locking

Design flow with Logic Locking





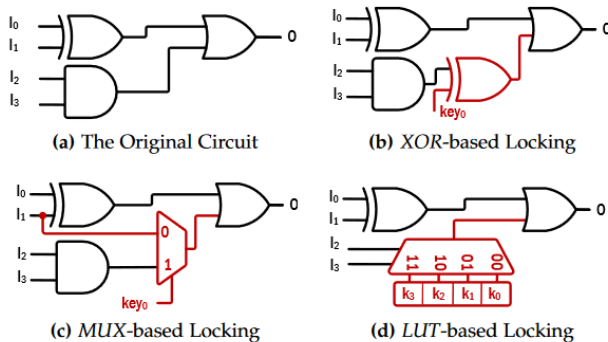
First Logic Locking Techniques (2008-2015)

- Insertion algorithms

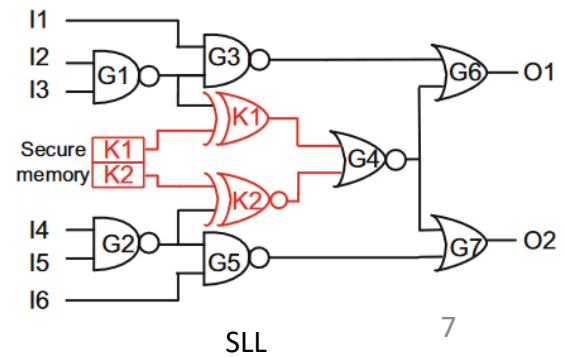
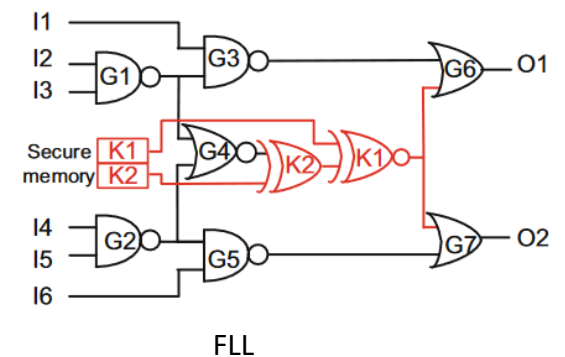
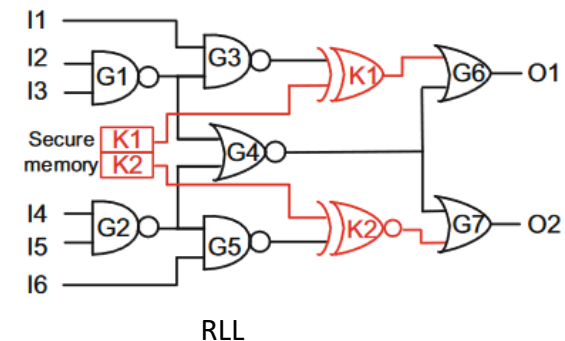
- RLL (Random Logic Locking) introduced by EPIC
- FLL (Fault Logic Locking) to maximize output corruption
- SLL (Strong Logic Locking) a response to the first LL attack

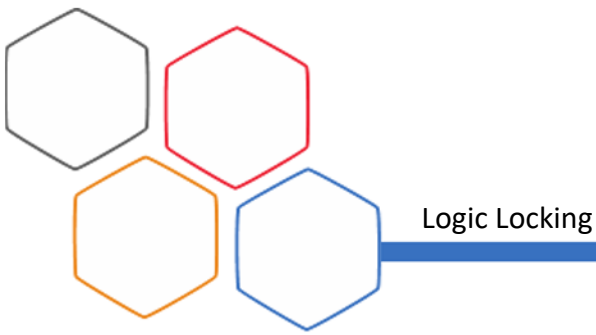
- Key « Gates »

- XOR/XNOR
- MUX's
- LUT's



Different entities insertion

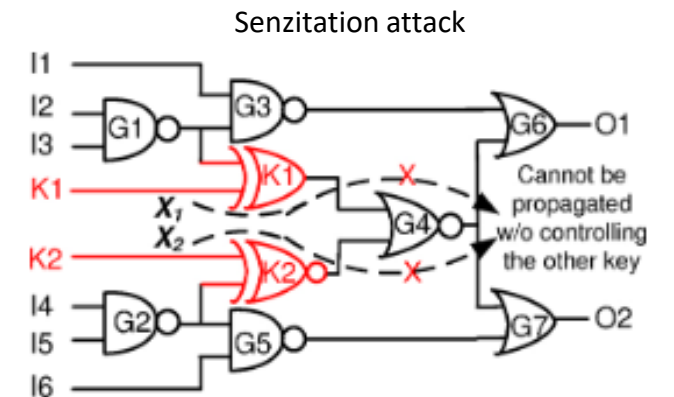
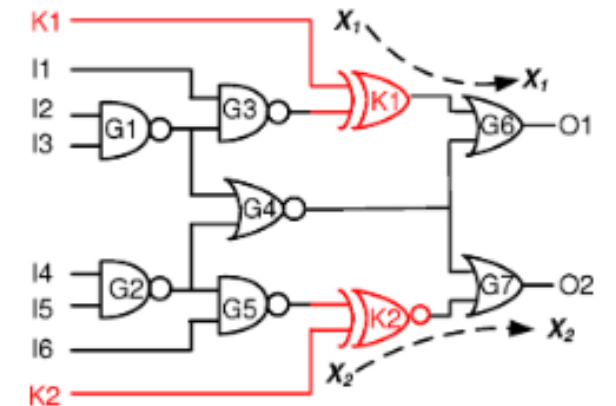




Attack and Threat Model

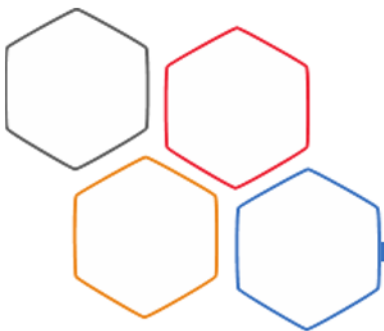
Attack on LL scheme → Retrieve the locking key

- The threat model
 - Functional IC and Locked netlist → Oracle Guided Attacks
- The first attack (Oracle Guided attack)
 - Sensitization attack [3]: Observe key bits on primary outputs
- The first counter-measure
 - Strong Logic Locking

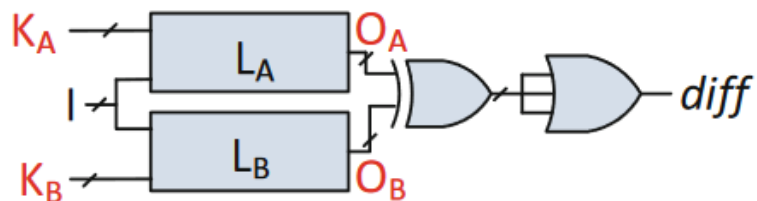


SLL

[3] J. Rajendran, Y. Pino, O. Sinanoglu and R. Karri, "Security analysis of logic obfuscation," *DAC Design Automation Conference 2012*, San Francisco, CA, USA, 2012, pp. 83-89, doi: 10.1145/2228360.2228377

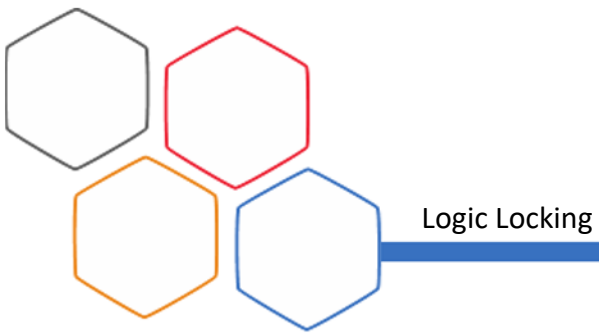


- Subramanyan et al [5]
- The attack flow (iterative process)
 - Construct Mitter circuit
 - Find Distinguishing Input Patterns
 - Refine key resarch Space



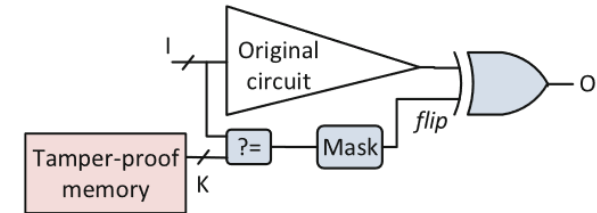
abc	Y	k0	k1	k2	k3	k4	k5	k6	k7	Incorrect keys identified
000	0	1	1	1	1	0	0	0	1	
001	0	0	1	1	1	0	1	0	1	
010	0	1	1	1	1	1	1	0	1	Iter 3 : other keys
011	1	1	1	1	1	0	1	1	1	
100	0	1	1	1	1	1	1	0	1	
101	1	1	1	1	1	1	1	1	0	
110	1	1	1	0	1	1	1	1	1	Iter 1 : k2
111	1	1	0	1	1	1	1	1	1	Iter 2 : k1

[5] P. Subramanyan, S. Ray and S. Malik, "Evaluating the security of logic encryption algorithms," 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 2015, pp. 137-143, doi: 10.1109/HST.2015.7140252.



The New LL Era

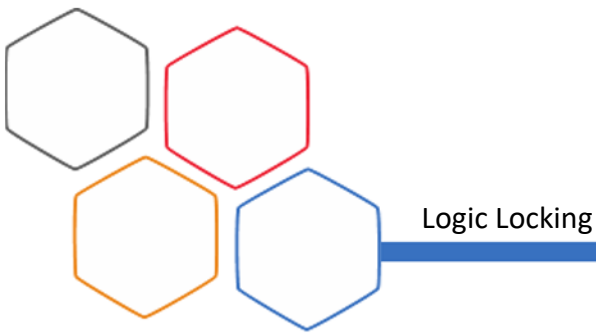
The point function LL (e.g. SAR-Lock)



- Weak output corruption →
 - Strong SAT resilience 😊
 - Black box usage 😞
 - Removal attack : Remove protection structure 😞

I	O	k0	k1	k2	k3	k4	k5	k6	k7
000	0	1	0	0	0	0	0	0	0
001	0	0	1	0	0	0	0	0	0
010	0	0	0	1	0	0	0	0	0
011	1	1	1	1	0	1	1	1	1
100	0	0	0	0	0	1	0	0	0
101	1	1	1	1	1	1	0	1	1
110	1	1	1	1	1	1	1	1	1
111	1	1	1	1	1	1	1	1	0

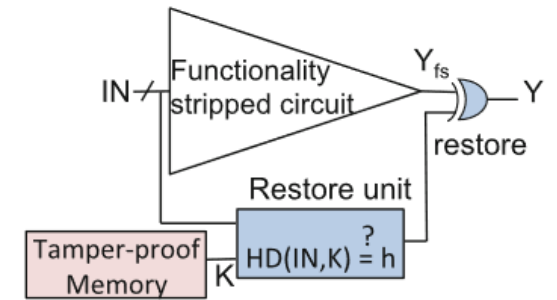
SAR-LOCK (K=110)



The New LL Era

The Corrupt And Correct (CAC) LL (e.g. SFLL-hd)

- Functionality Stripped Circuit
- Introduction of h parameter
 - More output corruption 😊
 - Less but still strong SAT-resilience 😊
 - Good compromise between SAT and black-box resilience 😊
 - Removal attack can not be applicable 😊
- Emergence of new types of attacks 😞
 - ML-based attacks
 - Scheme specified attacks



IN	Yfs	k0	k1	k2	k3	k4	k5	k6	k7	Y
000	0	0	1	1	0	1	0	0	0	0
001	0	1	0	0	1	0	1	0	0	0
010	1	0	1	1	0	1	1	0	1	0
011	1	1	0	0	1	1	1	1	0	1
100	1	0	1	1	1	1	0	0	1	0
101	1	1	0	1	1	0	1	1	0	1
110	1	1	1	0	1	0	1	1	0	1
111	0	0	0	0	1	0	1	1	0	1

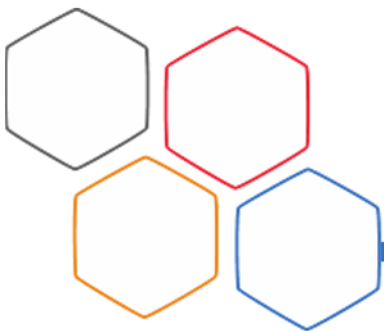
SFLL-HD (K=110, h=1)



→ Logic Locking

→ **SCA on Logic Locking**

→ Perspectives



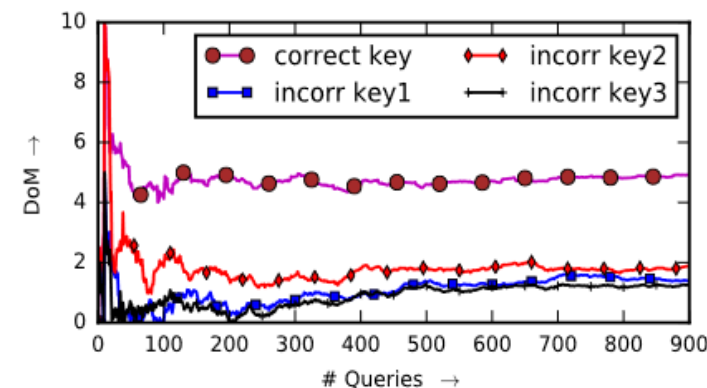
SCA on Logic Locking

What about Side Channel Attacks on pre-SAT LL schemes?

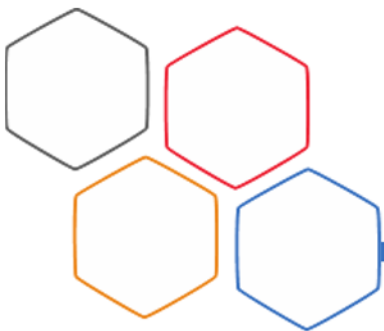
DPA attacks were realised against (RLL, FLL, and SLL) by [6] :

- Threat Model
 - Functionnal IC
 - Locked Netlist
- Iterative attack framework
 - Division of the netlist into logic cones
 - The decision function infered according to the PO's
 - The DoM on every subkey
- Simulated attack results
 - 60% of key-bits was resolved for circuits locked with 32 bits
 - 45% for circuits locked with 64 bits
 - Key aliasing induces ghost keys (High DoM for wrong keys)
 - Simulated power traces
 - Limitation on processing time

Name of cone	# key bits	List of key bits	Resolved?	# of key bits resolved
PO0	1	0	N	0
PO1	1	1	N	0
PO2	6	2,3,4,5,8,9	N	0
PO3	7	10,11,12,16,17,18,19	Y	7
PO5	8	6,7,13,14,15,29,30,31	Y	15
PO4	9	20,21,22,23,24,25,26,27,28	Y	24



[6] A. Sengupta, B. Mazumdar, M. Yasin, et O. Sinanoglu, « Logic Locking With Provable Security Against Power Analysis Attacks », *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 39, n° 4, p. 766-778, avr. 2020, doi: [10.1109/TCAD.2019.2897699](https://doi.org/10.1109/TCAD.2019.2897699).



Power analysis attacks on SFL-LL by [6]

- Threat Model

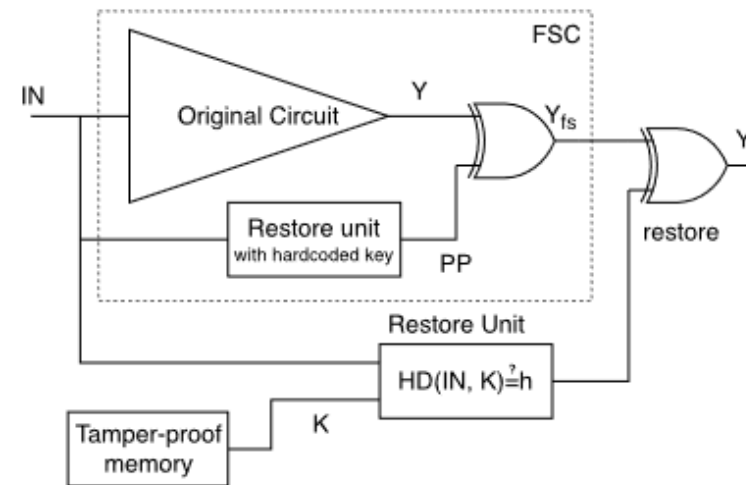
- Functionnal IC
- Locked Netlist

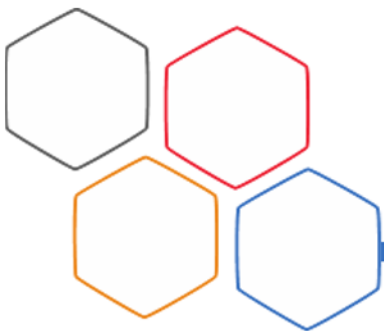
- Attack framework

- The decision function is the primary output bit of the circuit (Y)
- The DoM is calculated

- Attack results : DPA failed

- The PO Y is controlled from all key bits → brute force attack
- The corruption on Y for a few patterns → not significant to distinguish DoM values



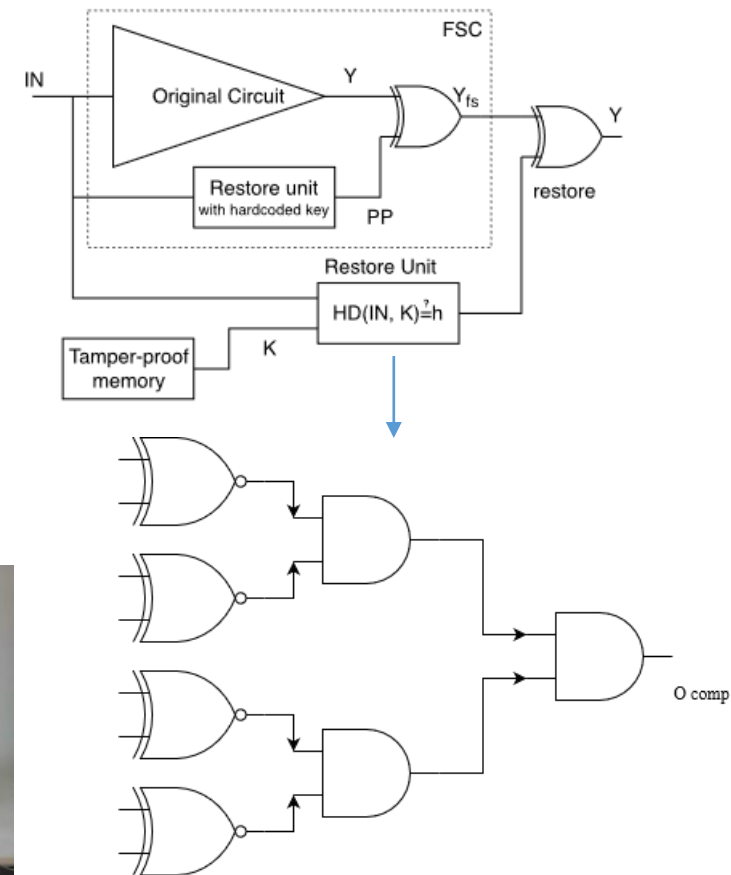
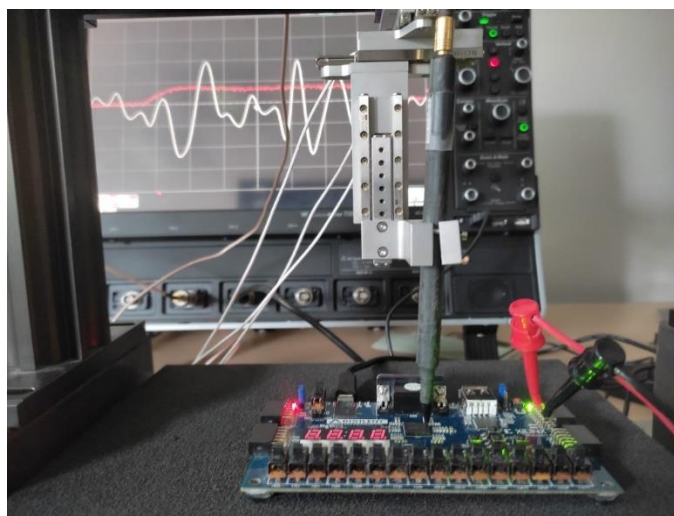
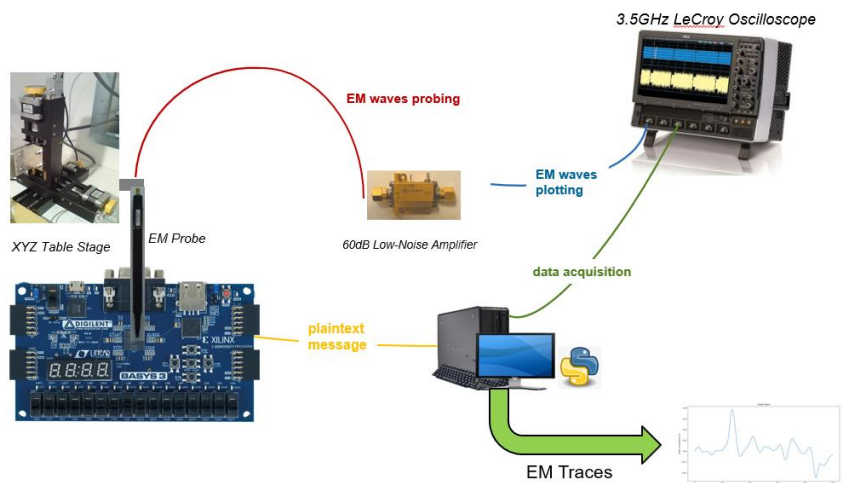


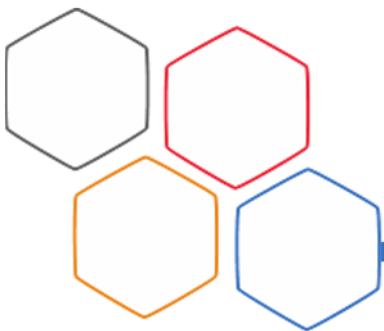
The Threat Model

- Functionnal IC (oracle)
- Locked Netlist

The attack framework

- The attack point will be the restore unit
- Divide and Conquer Methodology can be applied on the key
- The decision function will be the output of the sub-comparator

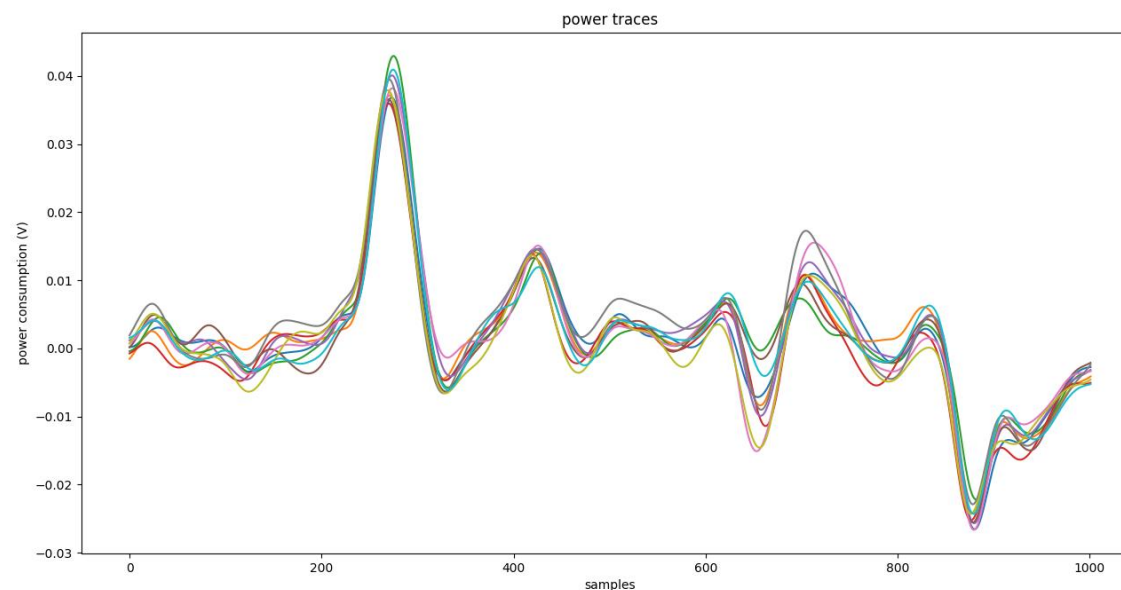


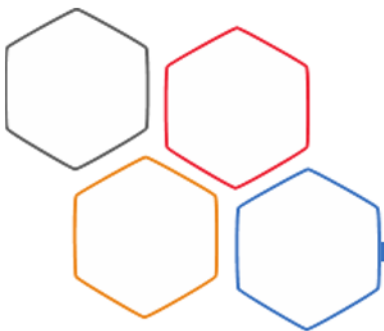


Power Traces Recording on the LIRMM/CNFM SCA platform

- Setup :

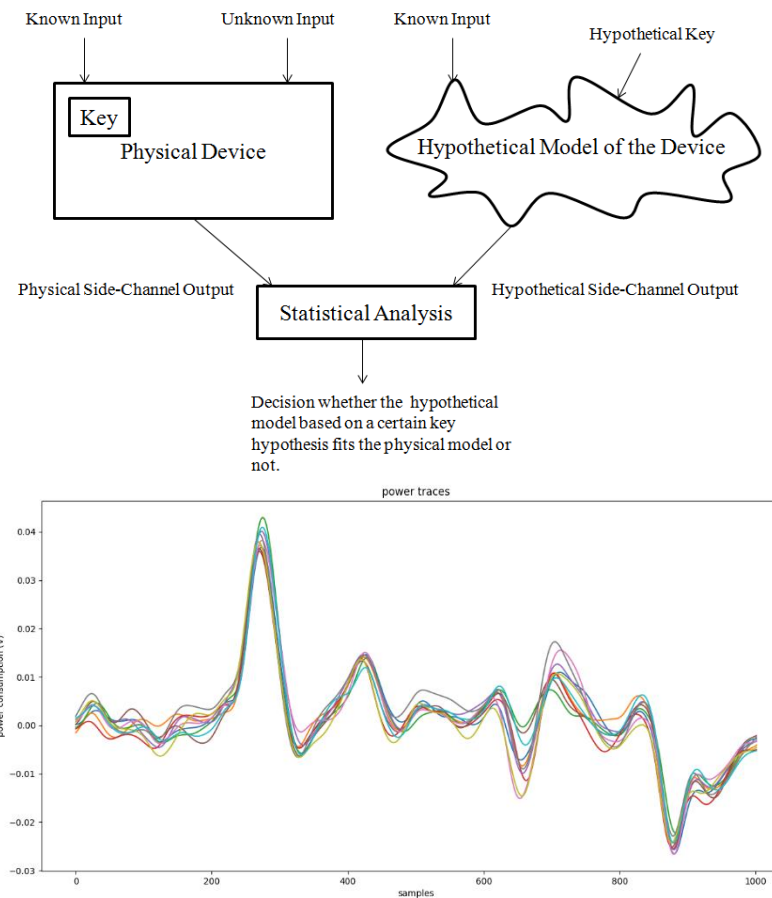
- Circuits : ISCAS circuits locked with SFLL-HD
- 1002 samples
- 2 clock cycles (update of data only on the first)
- Artix-7 FPGA
- Key stored on a register



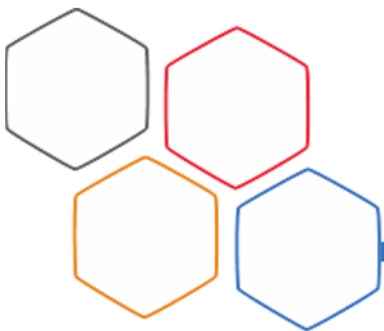


Attack of c432 with SFL-HD (h=0)

- Up to 200k traces
- DPA, CPA, MIA and template attacks
- No satisfying results



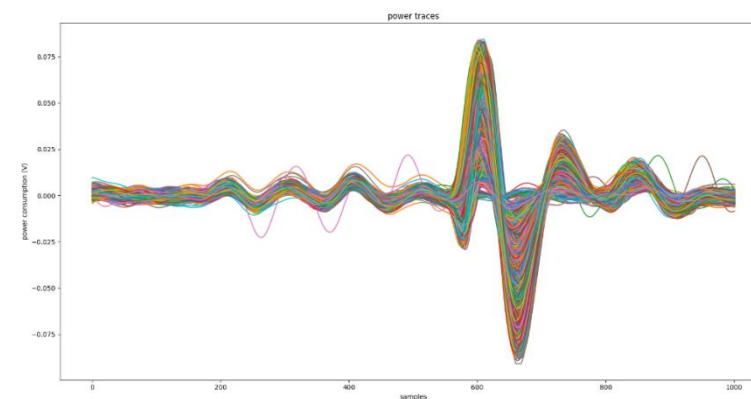
The Post-SAT schemes are really resilient against side channel attacks ?



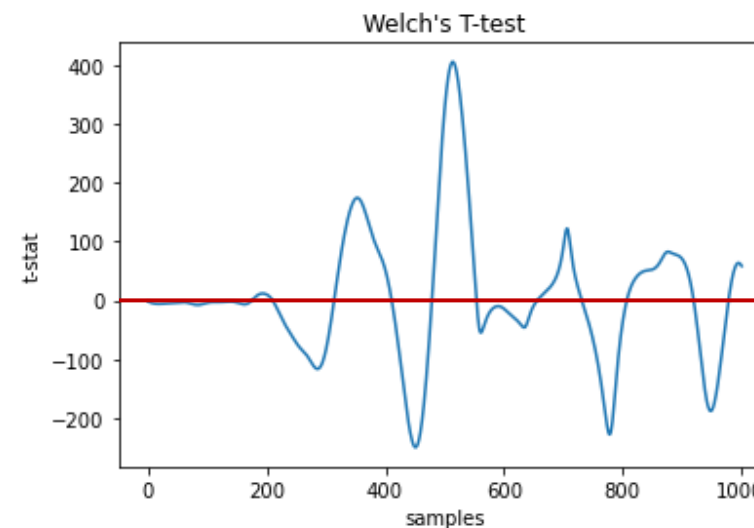
Leackage testing on DES circuit locked

- Leackage testing with Welch's T-test
- 50k traces with fixed correct key
- 50k traces with variable random keys
- The same input vectors were used

$$t = \frac{\overline{X1} - \overline{X2}}{\sqrt{\frac{S1^2}{N1} + \frac{S2^2}{N2}}}$$



Multiple DES power traces



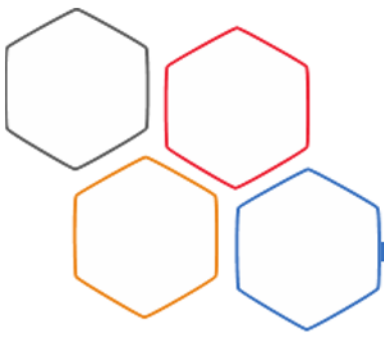
— Leakage limit :]-5,5[



→ Logic Locking

→ SCA on Logic Locking

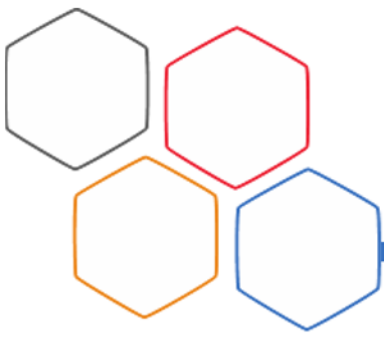
→ Perspectives



Futur Work

Perspectives

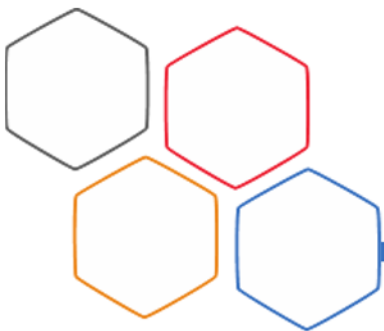
- Analysis of T-test Results
- Identifying the leakage sources
- Conduct the same leakage testing on other circuits with the same scheme
- DPA, CPA, MIA ...



Futur Work

Perspectives

- ➔ Simulation based leakage testing and SCA attacks (Cadence Joules, 28nm ST-FDSOI)
- ➔ Side Channel Attacks against other advanced LL schemes
- ➔ State of the art of other levels LL (RTL, Transistor, Layout)
- ➔ LL schemes with SCA resilience



Thank you all for listening

The SAFEST project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952252.

