# Full key recovery for advanced Logic Locking Schemes

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

# Full key recovery for advanced Logic Locking Schemes

Nassim Riadi, Florent Bruguier, Pascal Benoit, Sophie Dupuis, Marie-Lise Flottes
*LIRMM, Univ.Montpellier/CNRS*
Montpellier, France
first-name.last-name@lirmm.fr

***Index Terms*—Design-for-Trust, Logic Locking, Differential Power Analysis, Hardware obfuscation, VLSI Design.**

## I. Context and Motivation

Numerous frauds in the integrated circuit production have been made possible as the semiconductor industry has evolved over the decades from a vertical to a horizontal model with many entities involved in the design, integration, manufacturing, assembly and testing of a chip. Security and trust have since received particular attention for preventing piracy, copy, cloning, hardware Trojan insertion.

Design-for-Trust (DfTr) solutions [1] have thus emerged to thwart the theft of intellectual property during production, prevent any malicious modification during manufacturing and avoid copying after deployment on the market. Logic Locking (LL) consists in inserting extra logic into the design so that it becomes functional upon activation with a secret key defined by the designer. This approach received the most attention because it prevents piracy, overbuilding and reverse engineering and thus provides protection against the largest set of untrusted entities, SoC integrators, foundries, test facilities and end-users. The advanced LL schemes are until now considered as resilient to Differential Power Analysis (DPA) attacks [2], and authors claim that SAT-resilience implies DPA-resilience.

## II. DPA framework against Advanced schemes

We propose a framework for DPA attacks on the LL technique SFLL-HD$^0$ (Fig. 1) [3]. In SFLL-HD$^0$, the restore unit returns 1 when $HD(I, K) = 0$, so when the input data I corresponds to the secret key K. SFLL-HD$^0$ is selected among the different versions of the SFLL-HD approach because it provides the best resistance to the SAT attack.

Compared to previous work [2], we infer the DPA decision function by partitioning the RU and not the output node of the protect logic cone, this new strategy allows us to use divide and conquer methodology by targeting sub-parts of the restore-unit (Fig. 2). The power traces are obtained by Joules which rely on a VCD file obtained by simulation on a mapped netlist. The primary results shown in the table I are obtained by our first version of the framework. We could not achieve 100% due to ghost peaks. Classic solutions as NDPA [4] can not be applied, since Joules can't offer tune fined time samples for combinatorial circuits. So we enhance our framework by generating the VCD file according to POI (points of interest) and not for the whole circuit, this solution is equivalent to get the time slot from a scope. The new results are presented in table II.

This work is supported by the "France 2030" government investment plan managed by the French National Research Agency (ANR), under the project ARSENE (ANR-22-PECY-0004).

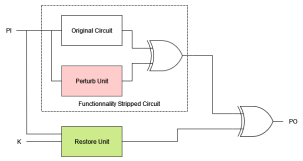


Fig. 1. SFLL-HD construction.

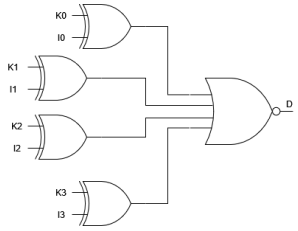


Fig. 2. Sub-part of the restore unit.

TABLE I
FIRST DPA RESULTS

| **benchmark** | c432 | c880 | c6288 | c3540 | 16 ADD |
|---|---|---|---|---|---|
| **bits retrieved** | 88.88 | 95 | 84.375 | 90 | 96.875 |
| **Power traces** | 42k | 80k | 46k | 64k | 34k |

TABLE II
ENHANCED DPA RESULTS

| **benchmark** | c432 | c880 | c6288 | c3540 | 16 ADD |
|---|---|---|---|---|---|
| **bits retrieved** | 100 | 100 | 100 | 100 | 100 |
| **Power traces** | $< 30k$ | $< 30k$ | $< 30k$ | $< 30k$ | $< 30k$ |

## References

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

[2] 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.

[3] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. V. Rajendran, O. Sinanoglu, Provably-Secure Logic Locking: From Theory To Practice, in ACM SIGSAC Conference on Computer and Communications Security, Dallas Texas USA: ACM, oct. 2017, p. 1601-1618.

[4] [1] J. Chen et al.,Normalized Differential Power Analysis - for Ghost Peaks Mitigationin 2021 IEEE International Symposium on Circuits and Systems (ISCAS)doi: 10.1109/ISCAS51556.2021.9401487.