STELLAR+:
Synthesis-friendly Signature Attenuation Countermeasure for EM and Power SCA

Stellar+ is a synthesis-friendly physical countermeasure which for the first time, brings the benefit of analog signature attenuation into digital domain and improves the state-of-the-art. Complete architecture is presented in fig. 1(a).
Stellar+ includes a ring oscillator which acts as local negative feedback and bypasses the instantaneous current to ground and stabilizes the node voltage V_{AES}. Moreover, ring oscillator frequency is an indication of its voltage. V_{AES} node voltage can be tracked using the frequency of ring oscillator. Hence, ring oscillator works as an input of global negative feedback loop which controls the number of current source slices to supply the encryption engine.
The detailed circuit diagram for global negative feedback is presented in fig. 1(b). A frequency divider is used to reduce power consumption of the loop without loss of functionality. An asynchronous counter counts the frequency divided oscillation and provides an estimation of V_{AES} node voltage. A decision circuit takes decision of turning on or off extra slices based on counter output. A detailed circuit functionality is explained in [1], [2].
The efficacy of signature attenuation is initially proposed by Das et. al showing promising initial results [3], [4]. Later, an ASIC version of it provides the proof-of-concept [5]. Initial state-of-the-art signature attenuation based countermeasures [5], [6] mostly use analog components to provide higher security, hence suffers from portability to different design and technology nodes. This work solves that problem, makes it synthesis-friendly and maximizes the uses of commercial tools in portability of different nodes.

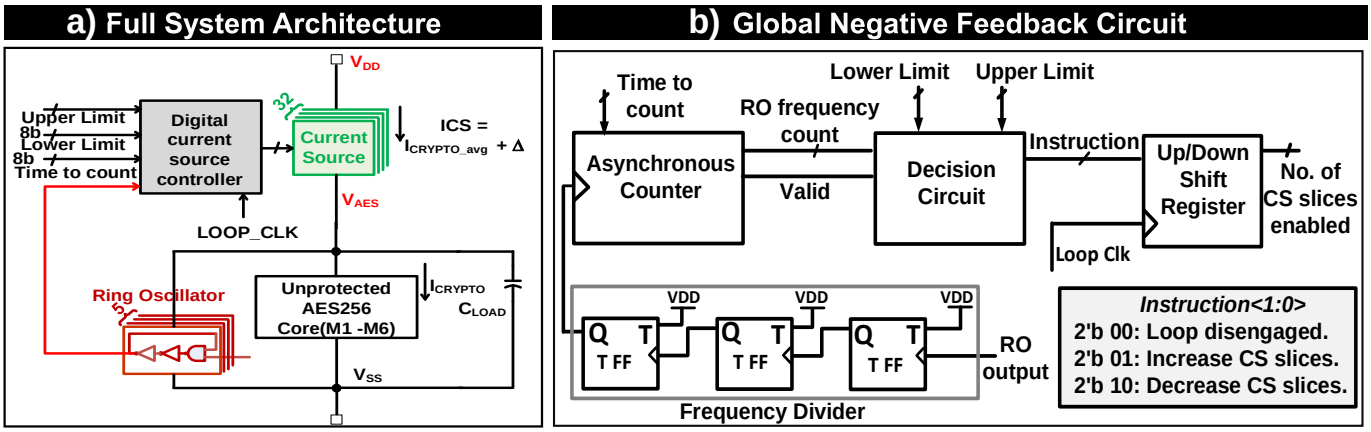

Fig. 1: a) Full system architecture for STELLAR+. b) Synthesizable global negative feedback loop.

Technology: Generic to any technology node. (For this example, 65nm TSMC CMOS technology)
Tools used: Cadence Virtuoso, Design Compiler, Cadence Innovus, Simvision, gcc.
Coding Language: Verilog, C
Ring oscillator is created by using a C script (ring_osc.c). It creates a file similar to ring_oscillator_61_stage.mapped.v. Based on stage requirement, script can be changed and oscillator of any stage can be generated. Note that, cell name for inverter will change based on technology nodes and processes. Hence, it should be accordingly changed in ring_osc.c. Script generated file can be directly used as an input to PnR tool to generate the layout automatically.
Frequency divider consists of 3 toggle flipflops. Toggle flipflop and and the frequency divider are located in the file frequency_divider.v.
Asynchronous counter is presented in oscillator_counter_v1.v. Moreover, it has one internal counter which keeps track of time_to_count (counter_v1.v).
Decision circuit & up/down shift register are integrated in a single design (up_down_counter_32b_average.v). It should be noted that loop_top_v2.v is the top file which includes asynchronous counter, decision circuit and up/down shift register

accordingly. All the files are located in current_source_controller folder.
Please cite the references if you use this repository.

REFERENCES

[1] Archisman Ghosh, Debayan Das, Josef Danial, Vivek De, Santosh Ghosh, and Shreyas Sen. 36.2 an em/power sca-resilient aes-256 with synthesizable signature attenuation using digital-friendly current source and ro-bleed-based integrated local feedback and global switched-mode control. In *2021 IEEE International Solid-State Circuits Conference (ISSCC)*, volume 64, pages 499–501. IEEE, 2021.

[2] Archisman Ghosh, Debayan Das, Josef Danial, Vivek De, Santosh Ghosh, and Shreyas Sen. Syn-stellar: An em/power sca-resilient aes-256 with synthesis-friendly signature attenuation. *IEEE Journal of Solid-State Circuits*, pages 1–1, 2021.

[3] Debayan Das, Shovan Maity, Saad Bin Nasir, Santosh Ghosh, Arijit Raychowdhury, and Shreyas Sen. ASNI: Attenuated Signature Noise Injection for Low-Overhead Power Side-Channel Attack Immunity. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 65(10):3300–3311, October 2018.

[4] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 62–67, May 2017.

[5] Debayan Das et al. 27.3 EM and Power SCA-Resilient AES-256 in 65nm CMOS Through >350× Current-Domain Signature Attenuation. In *2020 IEEE International Solid- State Circuits Conference - (ISSCC)*, pages 424–426, February 2020. ISSN: 2376-8606.

[6] Debayan Das, Josef Danial, Anupam Golder, Nirmoy Modak, Shovan Maity, Baibhab Chatterjee, Dong-Hyun Seo, Muya Chang, Avinash L Varna, Harish K Krishnamurthy, et al. Em and power sca-resilient aes-256 through $> 350\times$ current-domain signature attenuation and local lower metal routing. *IEEE Journal of Solid-State Circuits*, 56(1):136–150, 2020.