

Design space exploration of SABER in 65nm ASIC

Imran, Malik; Almeida, Felipe; Raik, Jaan; Basso, Andrea; Roy, Sujoy Sinha; **Pagliarini, Samuel Nascimento** ASHES '21 : proceedings of the 5th Workshop on Attacks and Solutions in Hardware Security 2021 / p. 85-90
<https://doi.org/10.1145/3474376.3487278>

High-level intellectual property obfuscation via decoy constants

Aksoy, Levent; Nguyen, Quang-Linh; **Almeida, Felipe; Raik, Jaan;** Flottes, Marie-Lise; Dupuis, Sophie; **Pagliarini, Samuel Nascimento** 2021 IEEE 27th International Symposium on On-Line Testing and Robust System Design (IOLTS) : Torino, Italy, 28-30 June 2021 2021 / p. 1-7 <https://doi.org/10.1109/IOLTS52814.2021.9486714>

High-speed SABER key encapsulation mechanism in 65nm CMOS

Imran, Malik; Almeida, Felipe; Basso, Andrea; Roy, Sujoy Sinha; **Pagliarini, Samuel Nascimento** Journal of cryptographic engineering 2023 / p. 461-471 : ill <https://doi.org/10.1007/s13389-023-00316-2> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Hybrid protection of digital FIR filters

Aksoy, Levent; Nguyen, Quang-Linh; **Almeida, Felipe; Raik, Jaan;** Flottes, Marie-Lise; Dupuis, Sophie; **Pagliarini, Samuel Nascimento** IEEE transactions on Very Large Scale Integration (VLSI) Systems 2023 / p. 812-825 : ill
<https://doi.org/10.1109/TVLSI.2023.3253641> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Ransomware attack as Hardware Trojan : a feasibility and demonstration study

Almeida, Felipe; Imran, Malik; Raik, Jaan; Pagliarini, Samuel Nascimento IEEE Access 2022 / p. 44827-44839
<https://doi.org/10.1109/ACCESS.2022.3168991> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

RESAA: A Removal and Structural Analysis Attack Against Compound Logic Locking

Almeida, Felipe; Aksoy, Levent; Pagliarini, Samuel Nascimento IEEE Transactions on Very Large Scale Integration (VLSI) Systems 2025 / p. 1348-1360 <https://doi.org/10.1109/TVLSI.2025.3534658>

RESAA: A Removal and Structural Analysis Attack Against Compound Logic Locking : [preprint]

Almeida, Felipe; Aksoy, Levent; Pagliarini, Samuel Nascimento arXiv.org 2025 / 12 p. : ill <https://doi.org/10.48550/arXiv.2409.16959>

Resynthesis-based attacks against logic locking

Almeida, Felipe; Aksoy, Levent; Nguyen, Quang-Linh; Dupuis, Sophie; Flottes, Marie-Lise; **Pagliarini, Samuel Nascimento** 2023 24th International Symposium on Quality Electronic Design (ISQED) : San Francisco, 5-7 April 2023 2023 / 8 p. : ill
<https://doi.org/10.1109/ISQED57927.2023.10129403> [Article at Scopus](#) [Article at WOS](#)

Side-channel attacks on triple modular redundancy schemes

Almeida, Felipe; Aksoy, Levent; Raik, Jaan; Pagliarini, Samuel Nascimento 2021 IEEE 30th Asian Test Symposium ATS 2021 : proceedings 2021 / p. 79-84 : ill <https://doi.org/10.1109/ATS52891.2021.00026> [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)