

#### **An area aware accelerator for elliptic curve point multiplication**

**Imran, Malik; Pagliarini, Samuel Nascimento;** Rashid, Muhammad Haroon 27th IEEE International Conference on Electronics Circuits and Systems, (ICECS) 2020, Glasgow, UK, Virtual Conference, November 23-25, 2020 : proceedings 2020 / 4 p  
<https://doi.org/10.1109/ICECS49266.2020.9294908>

#### **Chip-to-Chip authentication method based on SRAM PUF and public key cryptography**

Karageorgos, Ioannis; Isgenc, Mehmet Meric; **Pagliarini, Samuel Nascimento;** Pileggi, Larry Journal of hardware and systems security 2019 / p. 382–396 : ill <https://doi.org/10.1007/s41635-019-00080-y>

#### **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>

#### **Error sources in analog ASICs and ways for their minimization**

**Mihhailov, Juri** International journal of engineering and applied sciences (EAAS) 2013 / p. 32-41 : ill

#### **Hardware trojan insertion in finalized layouts : from methodology to a silicon demonstration**

**Perez, Tiago Diadami; Pagliarini, Samuel Nascimento** IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 2023 / p. 2094-2107 <https://doi.org/10.1109/TCAD.2022.3223846> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

#### **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](#)

#### **A pragmatic methodology for blind hardware trojan insertion in finalized layouts**

Hepp, Alexander; **Perez, Tiago Diadami; Pagliarini, Samuel Nascimento;** Sigl, Georg ICCAD '22: Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design 2022 / art. 69, p. 1-9 : ill <https://doi.org/10.1145/3508352.3549452> [Conference Proceedings at Scopus](#) [Article at Scopus](#) [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](#)

#### **SCALLER: standard cell assembled and local layout effect-based ring oscillators**

**Aljafar, Muayad J.; UI Abideen, Zain;** Peetermans, Adriaan; Gierlichs, Benedikt; **Pagliarini, Samuel** IEEE Embedded Systems Letters 2024 / p. 493 - 496 <https://doi.org/10.1109/LES.2024.3459730> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

#### **SCARF : securing chips with a robust framework against fabrication-time hardware trojans**

**Eslami, Mohammad; Ghasempouri, Tara; Pagliarini, Samuel Nascimento** IEEE Transactions on Computers 2024 / p. 2761-2775 <https://doi.org/10.1109/TC.2024.3449082> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

#### **SCARF : securing chips with a robust framework against fabrication-time hardware Trojans : preprint**

**Eslami, Mohammad; Ghasempouri, Tara; Pagliarini, Samuel Nascimento** arXiv.org 2024 / 14 p. : ill  
<https://doi.org/10.48550/arXiv.2402.12162>

#### **Side-channel Trojan insertion - a practical foundry-side attack via ECO**

**Perez, Tiago Diadami; Imran, Malik; Vaz, Pablo; Pagliarini, Samuel Nascimento** 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, May 22-28, 2021 : proceedings 2021 / 5 p. : ill <https://doi.org/10.1109/ISCAS51556.2021.9401481> [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)